量子コンピュータと量子通信 I

量子力学とコンピュータ科学

Michael A. Nielsen, Isaac L. Chuang 共著／木村達也 訳

Quantum Computation and Quantum Information

Ohmsha

両親と恩師に捧げる

まえがき

本書は量子計算と量子情報分野における主要な概念と技術に対する入門の役割を果たすものである．急速な進展と分野横断的な性格のために入門者がこの分野の最も重要な技術や成果を広く知ることが難しいのが現状である．

本書の目的は 2 つある．第 1 は量子計算と量子情報を理解するに必要なコンピュータ科学，数学及び物理学の基礎知識を提供することである．これら 3 分野の 1 つまたはそれ以上の分野における，学部学生と少なくとも同レベルの素養と，量子計算と量子情報を学ぶ希望を持つ読者を対象としている．本書の第 2 の目的は量子計算と量子情報に関する中心的成果を詳細に提供することである．全体を読み通すと読者は一般的教養として，あるいは量子計算と量子情報の研究への入門として，この刺激的分野における基本ツールと，その成果に対する実効ある理解力を身につけることができる．

本書の構成

本書の基本構成を図 1 に示す．本書は 3 部より成る．全体の基本姿勢として具体的なものから始めて抽象的内容に進むことを可能な限り心がけた．したがって，本書全体を通じて一般的理論を展開する前に実例を提示することとし，量子情報より先に量子計算を，一般的量子情報理論より先に具体的量子誤り訂正符号を扱うこととしている．

第 I 部では量子計算と量子情報分野における主要概念と成果を広く概観し，同分野を深く理解するに必要なコンピュータ科学，数学，物理学の基礎知識を学ぶ．1 章はこの分野の歴史的発展と基本概念を概観する入門的な章であり，その中で幾つか重要な疑問点を浮き彫りにする．その内容はコンピュータ科学や物理学の知識背景なしに理解できる構成となっている．より詳細を理解するに必要な基礎

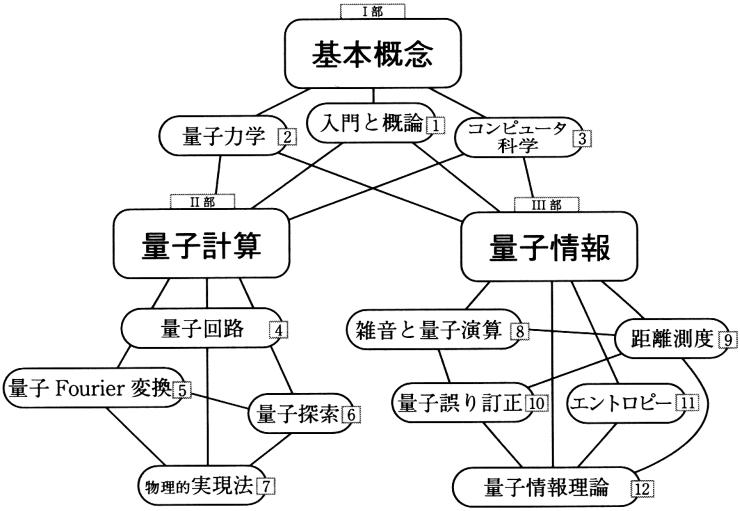


図 1: 本書の構成

知識は 2 章と 3 章で深められる．ここではそれぞれ量子力学とコンピュータ科学に関する基本概念を詳しく取り扱う．第 I 部の各章は読者の知識背景に応じて読み飛ばしても差し支えなく，量子力学やコンピュータ科学の基礎知識にギャップを感じたときに立ち戻ればよい．

第 II 部では量子計算について詳細に述べる．4 章で量子計算を行うに必要な基本要素について述べ，複雑な量子計算の応用に使う多くの基本操作を示す．5 章と 6 章は現在知られている 2 つの基本的量子アルゴリズムである量子 Fourier 変換と量子探索アルゴリズムについて述べる．5 章ではまた量子 Fourier 変換を使った素因数分解や離散対数問題の解法と，それらを応用した暗号について説明する．7 章では研究室で示された幾つかの実例を使って，量子コンピュータの一般的設計原理と望ましい物理的実現法の基準について述べる．

第 III 部は量子情報を取り扱う．量子情報とは何か，量子状態を使って如何に情報を表現し伝達するか，量子情報や古典情報の劣化を如何に表現しそれに対処するか等である．8 章は実世界の量子情報処理を理解するのに必要な**量子雑音**の性質と，量子雑音を理解するための強力な数学ツールである **量子演算形式**について述べる．9 章では 2 つの量子情報が似ているということが何を意味するかを，定量的に正確に表現できる量子情報の**距離測度**について述べる．10 章では雑音の影響

から量子計算を守るのに使う，量子誤り訂正符号について説明する．この章で紹介する重要な結果は**しきい値定理**であり，これは現実的雑音モデルにおいて**原理上**雑音が量子計算の深刻な障害にならないことを示す．11 章では**エントロピー**の情報理論的基本概念を紹介し，古典情報理論と量子情報理論の両方におけるエントロピーの性質を説明する．最後に 12 章で量子状態と量子通信チャンネルがもつ情報を運ぶ性能を議論し，古典的および量子的情報伝送や秘密情報伝送に対する，奇妙な興味ある性質について詳しく述べる．

本書を通じて数多くの演習と問題が提供されている．演習は基本的内容を確実に理解することを目的として，本文の途中に示されている．二三の例外を除きこれらの演習は数分で容易に解くことができる．問題は各章末尾に配置されており，本文中で十分に述べる余裕がなかった新しい興味ある材料を，読者に紹介するためのものである．しばしば問題は複数部分に分かれており，特定の深い思考方向に導くように意図されている．少数であるが本書刊行時点で解が示されていない問題もあり，その場合には課題中にその旨が述べられている．各章末にその章の主要結果のまとめを示すと共に，その章全体に関する引用文献を通して主要概念の発展経緯を示し，次のステップの資料を示唆する「歴史と参考資料」の節が設けられている．

本書の冒頭に詳細な目次があるので一覧して頂きたい．また用語と記号の手引きを載せたのでこれも読者の役に立つであろう．

巻末に 6 つの付録と参考文献および索引を収録した．付録 A では確率論の初歩に関する基本的定義，記号および結果をまとめた．この内容は読者に既知と思われるが参照の便宜のために掲載してある．同様に付録 B に読者の便宜のために群論の基本概念をまとめておいた．付録 C では量子計算のための重要な成果である Solovay-Kitaev の定理の証明を示した．この定理は任意の量子ゲートが有限個の量子ゲートで近似できることを示すものである．付録 D は素因数分解や離散対数に対する量子アルゴリズムや，RSA 暗号システムを理解するに必要な整数論の基本をまとめた．RSA 暗号システムについては付録 E で解説する．付録 F では量子計算と量子情報における最も重要な結果の 1 つであり，有名な強い劣加法性不等式 (strong subadditivity equality) のような重要なエントロピー不等式の先駆でもある，Lieb の定理の証明を示す．Solovay-Kitaev の定理と Lieb の定理の証明は非常に長いので，本文と別に扱うことにしたものである．参考文献では

本文中に引用した全資料のリストを収録した．迂闊にもこの引用から洩らしてしまった業績の研究者にはお詫び申し上げる．

量子計算と量子情報の分野は近年急速に進歩したため，全トピックスを望み通りの詳しさで網羅することができなかった．3 つの分野については特に述べておく必要がある．第 1 は**もつれの尺度**(entanglement measure) の話題である．本文で説明するようにもつれは量子テレポーテーション，高速量子アルゴリズム，量子誤り訂正等における重要な要素であり，手短に言えば量子計算と量子情報の優れたユーティリティ資源である．もつれの概念を新たな物理的資源として充実させ，その操作と有用性を左右する原理を見出している活発な研究グループが現在存在する．これらの研究は将来大いに有望ではあるが，本書で広範に記述した他の話題と同様な扱いをするにはまだ十分でないと我々は感じており，12 章で簡単に触れるに止めた．同様に分散量子計算（量子通信コンプレックスとも呼ばれる）は活発に発展している非常に有望な課題なので，本書の出版時点でもすでに時代遅れになっていることをおそれて取り扱うのを控えた．量子情報処理デバイスの実現も肥沃で魅力ある分野に発展してきたが，この話題については 1 つの章を当てるに止めた．明らかに物理的実現に関してもっと多くを述べることができるが，それを始めると関連する物理学，化学，工学の多くの分野に言及せざるを得ず，十分なスペースを割くことができなかった．

本書の使い方

本書は幅広くいろいろな使い方が可能である．量子計算や量子情報の特定のトピックスに関するショートコースから，全分野を網羅する 1 年間の講義に至るいろいろなコースの材料として使える．量子計算や量子情報について少し勉強してみようという方や，研究の最前線にまで知識を高めたいという方が個人的に勉強するのに役立つ．また，この分野の現役研究者にも参考資料として役立ててもらうのが著者の希望である．我々はこの分野に参加する研究者の入門用として特に価値を認められることを望んでいる．

個人読者の方々へ

本書は個人読者に読みやすいように工夫している．本文を通じて多くの演習が用意され，本文内容の理解度を自分でチェックできる．目次と章末のまとめを使ってどの章を深く学ぶべきかを容易に決められる．図1の関連分野ダイヤグラムは本書の材料をどういう順序でカバーするかを決める際に役立つであろう．

教師の方々へ

本書は広範囲のトピックスを網羅しているので，いろいろな種類のコースの材料として使うことができる．

量子計算の半年コース用教材ならば，クラスの学力に応じて1章から3章までの内容を選択し，次に量子回路の4章，量子アルゴリズムの5・6章，および物理的実現の7章の中の幾つかを選び，さらに量子誤り訂正を理解するために8～10章，特に10章に焦点を絞るとよい．

量子情報の半年コース用教材ならば，クラスの学力に応じて1章から3章までの内容を選択し，次に8～10章の量子誤り訂正，11章と12章の量子エントロピーと量子情報理論を選ぶとよい．

1年間のコースならば本書の全章を当て，さらに数章の「歴史と参考資料」から資料を選んで時間を充当することができる．また，量子計算と量子情報は学生の個人的研究テーマとしても最適である．

量子計算と量子情報の講義以外にも本書を利用して頂きたいのは，物理学の学生のための量子力学入門の講義である．従来の量子力学入門は偏微分方程式の数学手法に過度に依存してきたきらいがある．我々はこれがしばしば基本概念を不明確にすると信じている．量子計算と量子情報は数学的手法にあまり依存することなく，量子力学の基本概念と比類ない特徴を理解する格好の優れた思考場所を提供する．そのような講義では2章の量子力学入門に焦点を絞り，4章の量子回路に関する教材，5章と6章の量子アルゴリズムの抜粋，7章の量子計算の物理的実現，そしてIII部から好みに応じた部分を付け加えるとよい．

学生の皆さんへ

本書はできるだけ自己完結的に書かれている．主な例外は自分自身で納得するための議論を所々で省略したことであり，これらは通常演習の形で与えられている．本書を通読するに当たって全演習を少なくとも試みてみることをお勧めする．少数の例外を除いて演習は数分で解くことができる．もし多くの演習に多大の困難を感じるならば，もう一度立ち返って 1 つあるいはそれ以上の重要な概念を復習し直す必要性を示唆しているかも知れない．

さらに高度な資料

すでに述べたように各章末に「歴史と参考資料」の欄が設けてある．また読者が興味を持つかも知れない広範囲の参考資料も二三存在する．Preskill のすばらしい講義録 [Pre98b] は量子計算と量子情報に対して本書と少し異なる観点からアプローチしている．特定の主題に関する優れた解説論文を本書に現れる順に列挙すると，Aharonov の量子計算に関する解説 [Aha99b]，Kitaev の アルゴリズムと誤り訂正に関する解説 [Kit97b]，Mosca の量子アルゴリズムに関する学位論文 [Mos99]，Fuchs の量子情報の識別性と距離測度に関する学位論文 [Fuc96]，Gottesman の量子誤り訂正に関する学位論文 [Got97]，Preskill の量子誤り訂正に関する解説 [Pre97]，Nielsen の量子情報理論に関する学位論文 [Nie98]，Bennett，，Shor [BS98]，Bennett, DiVincenzo [BD00] による量子情報理論の解説がある．この他にも Gruska の著書 [Gru99]，Lo，Spiller，Popescu 編集になる解説論文集 [LSP99] が有用である．

正　誤

長大な文書にはしばしば誤りや欠落が伴う．本書もこの法則の例外ではない．もし，読者が誤謬を見つけたり，本書に関して異なるご意見をお持ちならば，qci@squint.org にメールを下さるようお願いする．見つかった誤りは本書の Web サイト http://www.squint.org/qci/ のリストに追加する．

謝辞

量子計算と量子情報について我々は数人の方々から決定的な影響を受けた．我々の考えを形成し洗練するのに大いに役立った多くの楽しかった議論に対して，MAN は Carl Caves，Chris Fuchs，Gerard Milburn，John Preskill および Ben Schumacher に，ILC は Tom Cover，Umesh Vazirani，Yoshi Yamamoto および Bernie Yurke に感謝する．

本書の執筆には非常に多くの人々から直接間接にご援助を頂いた．その一部をあげると，Dorit Aharonov, Andris Ambainis, Nabil Amer, Howard Barnum, Dave Beckman, Harry Buhrman, Caltech Quantum Optics Foosballers, Andrew Childs, Fred Chong, Richard Cleve, John Conway, John Cortese, Michael DeShazo, Ronald de Wolf, David DiVincenzo, Steven van Enk, Henry Everitt, Ron Fagin, Mike Freedman, Michael Gagen, Neil Gershenfeld, Daniel Gottesman, Jim Harris, Alexander Holevo, Andrew Huibers, Julia Kempe, Alesha Kitaev, Manny Knill, Shing Kong, Raymond Laflamme, Andrew Landahl, Ron Legere, Dabbie Leung, Daniel Lider, Elliott Lieb, Theresa Lynn, Hideo Mabuchi, Yu Manin, Mike Mosca, Alex Pines, Sridhar Rajagopalan, Bill Risk, Beth Ruskai, Sara Schneider, Robert Schrader, Peter Shor, Sheri Stoll, Volker Strassen, Armin Uhlmann, Lieven Vandersypen, Anne Verhulst, Debby Wallach, Mike Westmoreland, Cave Wineland, Howard Wiseman, John Yard, Xinlan Zhou, および Wojtek Zurek である．

本書をアイディア段階から出版までお世話になった Cambridge 大学出版の皆さんに感謝する．思慮深く情熱的な編集者 Simon Capelin はこのプロジェクトを 3 年以上にわたって指導し，Margaret Patterson は時宜を得て徹底した原稿編集をしてくれた．特に感謝する．

本書を執筆したのは，MAN が California 工科大学で Tolman Prize Fellow, Los

Alamos 国立研究所で T-6 理論宇宙物理学グループ研究員，および New Mexico 大学先端研究センタ研究員として在任中，一方 ILC が IBM Almaden 研究センタ研究スタッフ，Stanford 大学電気工学科助教授，California 大学 Berkeley 校コンピュータ科学部客員研究員，Los Alamos 国立研究所 T-6 理論宇宙物理学グループ研究員，California 大学 Santa Barbara 校理論物理学研究所客員研究員として在任中であった．本書の最終校正を完成した Aspen 物理学センタでの暖かいもてなしに感謝する．

MAN と ILC は NMRQC 研究イニシアティブのもとでの DARPA のご支援，陸軍研究オフィス下での QUIC 研究所によるご支援に深く感謝する．また，米国科学財団，米国国家安全局，海軍研究オフィスおよび IBM の寛大なご支援に感謝する．

訳者まえがき

本書は近年注目を集めている量子コンピュータと量子通信全般にわたる基本原理を懇切に述べた定本ともいうべき書である．原著の推薦文にはこの分野の発展に大きな貢献をした Michael Freedman, Charles Bennett, Peter Shor という錚々たる研究者が名を連ねており，学部レベル以上の理解力を持つ読者に向けて自己完結的な書物を書くことに成功しているとの評を与えている．この分野はすでに非常に大きくなりすべてをカバーすることはもはや困難になっているが，著者らは話題をよく選択してそれをわかりやすく説明している．

その大きな特徴は著者のまえがきにあるように，単純から複雑へ，実例から一般へ，具体から抽象へという姿勢を徹底して保っていることであり，理論主体の書でありながら読みやすく説明されている．ちなみに本文中に「直観」という言葉が実に百回以上も使われている．これは単に論理による説得ではなく，読者の論理的理解と直観的納得の整合を重視する著者の説明姿勢を端的に現わしている．

著者の一人 Michael A. Nielsen はオーストラリアのクイーンズランド大学の教授であり，ニューメキシコ大学，ロス・アラモス国立研究所，カリフォルニア工科大学等で研究業績をあげている．またもう一人の Isaac L. Chuang はマサチューセッツ工科大学の準教授であり，スタンフォード大学，カリフォルニア大学バークレー校，ロス・アラモス国立研究所，IBM アルマデン研究所等で研究業績をあげている．二人の研究論文は巻末の参考文献にそれぞれ 10 編以上リストアップされており，研究の第一線で活躍していることがわかる．

量子コンピュータや量子通信はコンピュータ技術や光ファイバ通信技術の未来の夢を示す方向として，またナノテクノロジーやフォトニクス技術の将来の進路を示す可能性の 1 つとして大いに期待され，科学技術先進諸国で多大のリソースが投入されて研究の推進がはかられている．この状況の中で，確固たる将来展望のもとに基本的事項をしっかりと記述した，本書のような書物の重要性が一層増

していると考えられる．このような意味で本書がわが国の学生，技術者を始め研究者や研究者を目指す多くの方々のお役に立つことができて，わが国のこの分野の研究発展に資することができれば，望外の幸せである．

翻訳に当たってはこの著者の姿勢を生かすよう留意したつもりである．さらに訳出にあたって著者のまえがきのある Web サイトに掲載された正誤にはすべて対応するとともに，翻訳時に見つかったその他の誤りもできるだけ修正しておいた．量子計算・量子情報の分野は数学・物理学・コンピュータ科学・通信工学・エレクトロニクス・フォトニクス・材料科学等，数多くの分野の境界領域であり，多くの分野の術語が入り交じって使われる．また，最先端分野に相応しくこの分野特有の新しい術語も生まれている．日本語への定着度が低い場合もあり，また特定の分野を背景とする読者は多少違和感を感じる場合もあるかも知れない．翻訳に伴ってこのような分野に見られる 1 つの問題点として，異なる英文術語が異なる領域で同一の和文術語に対応する場合がある．二三の例をあげると，基底（空間の base，対数の base，準位の ground），交換（commute，swap，exchange），可逆（invertible，reversible，reciprocal），指数（index，exponent），限界（bound，limit）等がある．文脈から判断できるようにするとともに，誤解のないように英術語を併記したところも多い．また和文と異なり英文での「以上」，「以下」はその数を含まない場合が多いことを付記しておく．

翻訳に当たって多くの方々にお世話になった．石原直氏，磯崎秀樹氏，向井孝彰氏，山本喜久氏に深く感謝する．また高柳英明氏，森田雅夫氏を始め NTT 物性科学基礎研究所の方々と NTT コミュニケーション科学基礎研究所の方々に多くの点で有益なご意見を頂いた．心からお礼を申し上げる．最後になったが出版に関してお世話になったオーム社出版部の方々に感謝する．

2004 年 12 月

訳者しるす

目　次

第 II, III 巻目次

第 II 巻 — 量子コンピュータとアルゴリズム —

第 III 巻 — 量子通信・情報処理と誤り訂正 —

用語と記号

量子計算と量子情報分野で共通に使われる用語と記号には，2 つあるいはそれ以上の意味を持つものがある．混乱を避けるためにここではこれら頻繁に使われる用語や記号を集め，本書での用法を併記する．

線形代数と量子力学

全ベクトル空間は特に断らない限り有限次元と仮定する．多くの場合にこの制約は不必要であるか，あるいは若干のテクニカルな操作により取り除くことができる．しかし一般にこの制約を設けることにより容易に理解することができ，結果を応用する際に用途が狭まることはない．

オペレータ (演算子，作用素，operator) A が**正のオペレータ** であるということは，すべての $|\psi\rangle$ に対して $\langle\psi|A|\psi\rangle \geq 0$ となることである．また**正の定符号オペレータ** A とは $|\psi\rangle \neq 0$ に対して $\langle\psi|A|\psi\rangle > 0$ となるオペレータである．オペレータの台 (support) は核 (kernel) と直交するベクトル空間であると定義される．これは Hermite オペレータ (Hermitian operator) に対して固有値が 0 でないオペレータの固有ベクトルが形成するベクトル空間を意味している．

記号 U（および，常時ではないがときどき V も）は総称的にユニタリーオペレータ (unitary operator) またはユニタリー行列 (unitary matrix) を表すのに用いる．H は通常量子論理ゲートの 1 つである Hadamard ゲート を表すのに用いるが，ときどき量子システムのハミルトニアン (Hamiltonian) を表す．この意味の違いは文脈より明らかである．

ベクトルは時に応じて，例えば

$$\begin{bmatrix} 1 \\ 2 \end{bmatrix} \tag{0.1}$$

のような列形式で書かれ，別のときには読み易いように行形式 (1, 2) で書くこともある．後者は列ベクトルの略記法と理解してほしい．通常，q ビットとして用いられる 2 準位システムに対して状態 $|0\rangle$ をベクトル (1, 0) で表し，状態 $|1\rangle$ を (0, 1) で表す．また我々は Pauli の σ 行列 (Pauli σ matrix) を通常用いられる通りに定義する．次に述べる「よく用いられる量子ゲートと回路記号」の項を参照されたい．最も重要なことは Pauli の σ_z 行列に対する慣行は $\sigma_z|0\rangle = |0\rangle$，$\sigma_z|1\rangle = -|1\rangle$ であり，一部の物理学者の直観と逆になっている（通常コンピュータ科学者や数学者はそうしない）．この不一致の原因は物理学者は σ_z の $+1$ 固有状態をいわゆる「励起状態」と規定し，多くの人がこれを本書で採用した $|0\rangle$ ではなく $|1\rangle$ と表すのが自然だと考えるからである．我々の選択は線形代数の行列要素における通常の指数と一致するものであり，σ_z の第 1 列と $|0\rangle$ に及ぼす σ_z の作用とを一致させ，第 2 列を $|1\rangle$ に及ぼす作用と一致させる．この選択は量子計算と量子情報の分野を通じて広く用いられている．Pauli の σ 行列に対する通常の記号 σ_x，σ_y，σ_z に加えて，これらの代わりに記号 σ_1，σ_2，σ_3 および 2×2 の単位行列 σ_0 を用いることも便利である．しかし，我々は σ_0，σ_1，σ_2，σ_3 に代えてそれぞれ記号 I，X，Y，Z を頻繁に用いる．

情報理論と確率

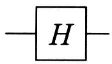
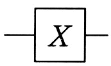
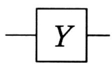
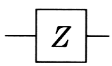
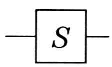
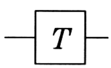
優れた情報理論家にふさわしく特に断らない限り対数は常に 2 を基底とする．$\log(x)$ は 2 を基底とする対数を表し，稀にしか使わないが $\ln(x)$ は自然対数を表す．**確率分布**(probability distribution) という用語は $p_x \geq 0$ かつ $\sum_x p_x = 1$ であるような実数 p_x の有限集合を表す．正のオペレータ B に対する正のオペレータ A の相対エントロピー は $S(A \| B) \equiv \mathrm{tr}(A\log A) - \mathrm{tr}(A\log B)$ で定義される．

その他

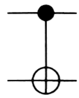
$\oplus$ は 2 を法とする和 を表す．本書を通じて 'z' は [zed] と発音する．

よく用いられる量子ゲートと回路記号

量子回路の設計に有用なユニタリー変換を表すのに，幾つかの図式的な記号がよく使われる．読者の便宜を図るためにそれらを集めて示しておく．ユニタリー変換の行と列は，00 ...0，00 ...1，から 11 ...1 というように左から右へ，上から下へと並べられ，最後の数字が最も重要でないビットを表す．$e^{i\pi/4}$ は i の平方根であり，したがって $\pi/8$ ゲートは，Pauli-Z ゲートの平方根である位相ゲートの平方根である．

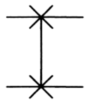
Hadamard ゲート		$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X ゲート		$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y ゲート		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z ゲート		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
位相ゲート		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ ゲート		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

制御 NOT ゲート



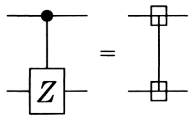
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

交換ゲート



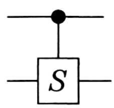
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

制御 Z ゲート



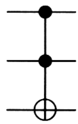
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

制御位相ゲート



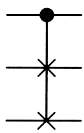
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{bmatrix}$$

Toffoli ゲート



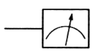
$$\begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{bmatrix}$$

Fredkin ゲート
（制御交換ゲート）



$$\begin{bmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&0&1&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1 \end{bmatrix}$$

測定



$|0\rangle$ と $|1\rangle$ への射影

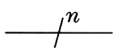
q ビット

単一 q ビットの配線
（時間は左から右へ経過）

古典ビット

単一の古典ビットの配線

n 個の q ビット



n 個の q ビットの配線

第I部

基本概念

第1章　概　論

科学はその時代の最も大胆な形而上学的理論を提供する．それはもし我々が夢見て，発見を求め，説明し，再び夢見ることを通して何度も新たな環境に飛び込むならば，世界がやっと明確になり宇宙の真の不思議が把握できるという信念に駆られて，人間のみが作れる構築物である．こうしてその不思議が互いに関連付けられ意味がわかってくる．— Edward O. Wilson

情報は物理的である．— Rolf Landauer

量子計算と量子情報の基本概念は何か？ その概念は如何にして生まれてきたか？ どのような用途があるか？ 本書ではそれらをどのよう提示するか？ この1章の目的は，量子計算と量子情報分野の描像を奔放な筆遣いで描くことによってこれらの疑問に答えることである．意図するところは，この分野の主要概念の基本理解と発展の経緯を伝え，読者が本書の内容にどのようにアプローチするかを決める手助けをすることにある．

まず最初の1.1節で量子計算と量子情報が発展してきた歴史的経緯を説明することから始める．この章の他の節では，この分野の基本概念を取り上げて手短に説明する．すなわち，量子ビット（1.2節），量子コンピュータ・量子ゲートおよび量子回路（1.3節），量子アルゴリズム（1.4節），量子情報処理の実験（1.5節），ならびに量子情報と通信（1.6節）である．

説明途上で本章で扱う基礎的数学を用いて，量子テレポーテーションや幾つかの簡単な量子アルゴリズムのような，例示的で取りつきやすい新事実を示すことにする．本章の内容はそれだけで独立しており，コンピュータ科学や物理学の素

養なしで理解できるように考えられている．さらに進むと，後の章で一層深い議論への指針を与え，参考文献や次のステップへの書物を示す．

読んでいくうちに難しくなればそこは読み飛ばして，理解できるところまで進んでもかまわない．ところによっては後になって初めて完全に説明できるような技術的専門用語を使わざるを得なかった部分も少数ながらある．当面はそれを受け入れてすべての用語を完全に理解してから再度戻ってくればよい．この最初の章で重要なのは大まかな描像を描くことであり，細部は後で補えばよい．

1.1　全体の展望

量子計算と量子情報は量子力学的システムを用いて達成できる情報処理の学問である．一見かなり簡単で明瞭そうに見えるであろう．しかし多くの単純であるが奥深い概念と同様に，量子力学的システムを用いた情報処理を着想するには長い時間がかかった．それがなぜかを見るには，時代を遡って量子計算と量子情報の基本概念に貢献した分野 — 量子力学，コンピュータ科学，情報理論，および暗号 — を 1 つずつ見ていかねばならない．これらの分野を手早く見て回るには，量子計算と量子情報に合流することになった別々の分野の様子を知るために，読者自身が最初は物理学者，次に計算機学者，次に情報理論家，最後に暗号技術者のつもりになってもらいたい．

1.1.1　量子計算と量子情報の歴史

我々の歴史は科学分野において予想できなかった革命が進行した 20 世紀初頭に始まる．物理学において一連の危機が訪れていた．問題は当時の物理学—今でいう**古典物理学** (classical physics)— の理論が，無限大のエネルギーを含む「紫外域の破局」や電子が原子核に向かって落ち込んで行くらせん運動というような，不条理な予測をし始めたことにあった．最初そのような問題には古典物理学に**その場しのぎ**の仮説を追加してしのいでいたが，原子や放射に関する理解が進むにつれて，このような説明の試みは複雑で困難になってきた．混乱が 4 半世紀も続き 1920 年代のはじめに危機が頂点に達して，**量子力学** (quantum mechanics) の近代的理論が誕生した．それ以来量子力学は科学に不可欠な位置を占め — 原子

の構造，星の内部の核融合，超伝導体，DNA の構造，自然界の素粒子を含む — 太陽の下と内部のあらゆるものを説明することに成功した．

量子力学とは何か？ 量子力学は物理学理論を構築するための数学的な枠組み，もしくは一組の法則である．例えば，原子と光の相互作用を素晴らしく正確に記述する，**量子電気力学** (quantum electrodynamics) という理論物理学がある．量子電気力学は量子力学の枠組みの中で構築されているが，その中には量子力学では決定できない具体的法則が含まれている．量子力学と量子電気力学のような特定の物理学理論との関係は，どちらかというとコンピュータのオペレーティングシステムと具体的アプリケーションソフトウェアとの関係に似ている．オペレーティングシステムは基本的パラメータや操作モードを用意するが，特定のタスクはアプリケーションが行うように残されている．

量子力学の法則は簡単であるが専門家にとっても非直観的であり，量子力学をよりよく理解したいという物理学者の長い間の夢の中に，量子計算と量子情報の起源が見出される．有名な量子力学の批判者であった Albert Einstein は，彼が発見するのに尽力した理論と折り合いをつけることなく，鬼籍に入ってしまった．以来幾世代もの物理学者が口に合う料理に調理すべく，量子力学の予測と格闘してきた．量子力学に対する我々の直観を研ぎすますツールを開発して，その予測を我々にとってわかりやすいものにすることが，量子計算と量子情報の目的の 1 つである．

例えば, 1980 年代初頭に量子効果を用いて信号を光より速く送ること — Einstein の相対性理論により絶対に禁じられていること — が可能かという疑問が提起された．この問題の答えは未知量子状態のクローン（コピー）を作ることが可能かどうかで決まることがわかった．もしも**クローン** (clone) が作られれば量子効果を用いて光速より速く信号を送ることができるであろう．しかしながら（読者の前にある言葉とそれがどこから来たかを考えるとすぐわかるように）古典情報ではいとも容易であるが，量子力学では一般にクローンを作ることが可能でないことがわかった．1980 年代初期に発見されたこの**非クローン化定理** (複製不可能定理，no-cloning theorem) は初期の量子計算と量子情報における成果である．それ以来非クローン化定理は精密化され，今では量子クローン化デバイスが（当然不完全にではあるが）どこまでうまく動作するかまで理解できる概念上のツールになっている．さらに進んで，このツールは量子力学の他の側面を理解するのに

用いられている．

これに関連して量子計算と量子情報の発展に貢献した要素は，1970 年代に行われた**単一量子システムを完全に制御**する試みであった．1970 年代以前の量子力学の応用は，膨大な数の量子システムを含むかさばった試料を全体として制御するのが普通であり，個別の量子システムを直接取り扱うものではなかった．例えば，超伝導は実に見事に量子力学的に説明できる．しかし超伝導体は（原子のスケールに比べて）莫大な伝導性金属を含んでおり，超伝導体を構成する各量子システムに立ち入ることができないので，量子力学的側面の幾つかが探れるにすぎない．粒子加速器のようなシステムでは，ある範囲で各量子システムに立ち入ることができるが，これも個別の構成システムについてはほとんど制御できない．

1970 年代以後，単一量子システムを制御する多くの技術が開発された．例えば，単一原子を捕らえる「原子トラップ」法が開発され，外界から原子 1 個を隔離して，信じられないほどの正確さで多くの異なる側面からその振る舞いを探索することができる．走査トンネル顕微鏡は単一原子を自由に動かし，意のままに原子の列を作ることができる．単一電子の移動で動作する電子デバイスも実証された．

なぜ単一量子システムを完全に制御しようとあらゆる努力を傾注するのか？ 多くの技術的理由を脇に置いて純科学的理由に限ると，研究者はこれを虫の知らせで行ってきたというのが主な答えである．自然界の新たな領域を探る手法が開発されたときに，しばしば最も深い科学上の洞察が現れる．例えば，1930 年代と 1940 年代の電波天文学の発見によって，銀河系星雲の中心，パルサー，クエイサー等の一連の華々しい発見がなされた．種々のシステムの冷却法を見出すことによって低温物理学は目を見張る成功を収めた．同様に新しい予期しない現象の発見を目指して単一量子システムの完全制御法を手に入れることによって，我々は手つかずの自然領域を探索しているのである．今我々はこの方向に沿って最初の一歩を踏み出したところであり，すでに二三の興味深い驚きがこの領域で見出されている．単一量子システムを一層完全に制御し，さらに複雑なシステムに拡張できると，他にどんな発見ができるであろうか？

量子計算と量子情報は当然このプログラムに適合する．この分野は単一量子システムをよりうまく操作する方法を工夫する人々に，いろいろ困難な挑戦的課題を数多く提供し，最も興味ある実験の方向に向けて新たな実験技術の開発を刺激し指針を与える．逆にもし量子計算と量子情報への応用に向けて量子力学の能力

を利用したいならば，単一量子システムの制御能力は必要不可欠なものである．

このような強い興味にもかかわらず，これまで量子情報処理システムを構築する努力はまだあまり大きな成功は収めていない．数個の量子ビット—あるいは，**q ビット**(qubit) — に数十回の演算を行わせることができる小さな量子コンピュータが量子計算の現状を表しているにすぎない．**量子暗号** (quantum crypyography) のプロトタイプ実験 — 長距離にわたって秘密に通信を行う方法 — が実証され，実世界の応用に有用かも知れないというレベルにある．しかし，大規模量子情報処理の実現は将来の物理学者や技術者にとって大きな挑戦として横たわっている．

量子力学から目を転じて，もう 1 つの 20 世紀の偉大な知的勝利であるコンピュータ科学に注目しよう．コンピュータ科学の起源は歴史の深みに埋もれてしまった．例えば，楔形文字の書板によれば Hammurabi（紀元前 1750 年頃）の時代に，バビロニア人はかなり高度なアルゴリズムの概念を有しており，その多くの概念はおそらくもっと古い時代にさかのぼると言われている．

近代的コンピュータ科学を具現したのは，偉大な数学者 Alan Turing により発表された 1936 年の注目すべき論文である．Turing は今日我々がプログラムで制御できるコンピュータと呼ぶ抽象的概念 — 彼の名誉を記念して **Turing 機械** (Turing machine) と呼ぶモデル — を詳しく発展させた．Turing は如何なる他の Turing 機械もシミュレートできる**普遍的 Turing 機械** (万能 Turing 機械，universal Turing machine) が存在することを示した．さらに，彼は普遍的 Turing 機械がアルゴリズムを用いてタスクの実行を**完全に捕捉**できると主張した．つまり，もしアルゴリズムが**任意の**ハードウェア—例えば現代のパソコン—上で実行できるなら，パソコンのアルゴリズムと全く同じタスクを普遍的 Turing 機械で正確に実行できる等価アルゴリズムが存在する．この主張は Turing ともう一人のコンピュータ科学の先駆者 Alonzo Church に敬意を表して **Church-Turing の提唱** (Church-Turing thesis) と呼び，**ある物理的デバイス**上でどんなクラスのアルゴリズムが実行できるかという物理的概念と，普遍的 Turing 機械の厳密な数学的概念とが等価であると主張している．この提唱は広く受け入れられて，コンピュータ科学の豊かな理論発展の基礎となった．

Turing の論文から程なく電子部品で組み立てられた最初のコンピュータが開発された．John von Neumann はコンピュータが普遍的 Turing 機械として完全な機能を有するために，必要な全部品の具体的組み立て方を示す簡単な理論モデ

ルを開発した．ハードウェアの開発は John Bardeen，Walter Brattain および Will Shockley がトランジスタを発明した 1947 年に離陸した．それ以後ハードウェアはめざましい早さで処理能力を向上し，1965 年に Gordon Moore が提唱した **Moore の法則** (Moore's law) — コンピュータ処理能力はコストを一定としてほぼ 2 年で 2 倍になる — として知られる割合で成長を遂げた．

驚くべきことに Moore の法則は 1960 年以後数十年にわたって近似的に成立してきた．それにもかかわらず多くの人たちは，この夢のような傾向が 21 世紀の最初の 20 年のいつかで終わると予測している．従来のコンピュータの製作技術は微細化の基本的困難によって失速し始めている．電子デバイスの小型化が進むにつれて，量子効果により機能が損なわれ始めているのである．

Moore の法則が破綻する問題に対処する究極的な解決法は，異なる計算パラダイムに移行することである．古典物理学に代わって量子力学を用いて計算を行うという発想に基づく量子計算理論によって，そのパラダイムの 1 つが用意されている．通常のコンピュータを用いて量子コンピュータをシミュレートできるが，シミュレーションを**効率良く**行うことは不可能であることがわかってきた．したがって，量子コンピュータは古典コンピュータに比べて速度の点で本質的に有利である．この速度の優位性は本質的なものであり，如何に古典コンピュータが考えられる限りの進歩をしようとも，古典コンピュータと量子コンピュータ間の計算性能のギャップは**克服できない**と多くの研究者が信じている．

量子コンピュータのシミュレーションが「効率的」か「非効率的」かは何を意味するのか？ この疑問に答えるに必要な主要概念の多くは量子コンピュータの概念が生まれる前から発明されていた．特に**効率的**アルゴリズムとおよび**非効率的**アルゴリズムの概念は**計算量** (computational complexity) の分野で数学的に精密化された．おおまかに言えば，効率的アルゴリズムとは解かれる問題のサイズの多項式の時間で働くものである．これに対して非効率的アルゴリズムは超多項式 — 典型的には指数関数 — の時間を必要とする．1960 年代後期から 70 年代初期にかけての見解は，Turing 機械を用いたシミュレーションによりある計算モデルで効率的に解ける問題は Turing 機械モデルで効率的に解けるという意味で，あたかも Turing 機械の計算モデルが他の如何なるモデルと少なくとも同等に高い能力を持つかのように認識されていた．この見解は強化された Church-Turing の提唱として表された：

> 如何なるアルゴリズムも Turing 機械を使って効率良くシミュレートできる．

強い Church-Turing の提唱における主な強化点は**効率良く**という言葉である．もしも強い Church-Turing の提唱が正しければ，アルゴリズムの実行に如何なるタイプのマシンを使おうとも，そのマシンは標準的 Turing 機械で効率良くシミュレートできることを意味する．与えられた計算タスクが効率良く実行できるかどうかを解析する目的には，Turing 機械による計算モデルの解析に話を限ってもよいということを意味しているので，この強化は重要である．

強い Church-Turing の提唱に対する 1 つの挑戦は**アナログ計算** (analogue computation) 分野から現れた．Turing の時代以来多くの異なる研究チームが Turing 機械が効率的解を持たないと信じられている問題を，あるタイプのアナログコンピュータで効率的に解けることに着目した．一見これらのアナログコンピュータは強い Church-Turing の提唱に反しているように見える．アナログ計算にとって不幸なことにアナログコンピュータに存在する雑音に関して現実的仮定を設けると，すべての既知の事例においてその計算能力は消滅し，Turing 機械で効率良く解けない問題はアナログコンピュータでも効率良く解けないことがわかった．計算モデルの効率を評価するには現実的雑音を考慮しなければならないというこの教訓は，初期の量子計算と量子情報に対する大きな挑戦の 1 つであった．この挑戦は**量子誤り訂正符号** (quantum error-correcting code) と**耐故障性量子計算** (耐誤り発生量子計算，fault-tolerant quantum computation) の理論を開発することで退けられた．したがって，量子計算はアナログ計算と違って原理上有限の雑音に対して耐性を持ち，かつ計算上の利点を保っている．

強い Church-Turing の提唱に対する最初の重要な挑戦は 1970 年代半ばに現れた．Robert Solovay と Volker Strassen は**確率的アルゴリズム**(randomized algorithm) を用いて，整数が素数であるか合成数であるかがテストできることを示したのである．すなわち，Solovay-Strassen の素数テストは乱数をアルゴリズムの**本質的部分**として用いた．このアルゴリズムでは与えられた整数が素数であるか合成数であるかを確実に決定する代わりに，その整数が**多分**素数であるかあるいはそうでなければ**確実に**合成数であることを決定する．Solovay-Strassen テストを数回繰り返せば，整数が素数であるか合成数であるかをほとんど確実に決

めることができる．Solovay-Strassen テストが提案されたときには素数を決定する効率的な決定論的方法が知られていなかったし，本書執筆時点でもまだ知られていないので，このテストは特に重要な意味を持っていた．したがって，この乱数発生器に接続できるコンピュータは，従来の決定性 Turing 機械が効率的解を持たない計算タスクを，効率的に実行できるようにみえた．この発見によって他の確率的アルゴリズム探索が刺激され，高い成果が得られると共に盛んな研究分野へと花咲いていった．

確率的アルゴリズムで効率良く解けるが，決定性 Turing 機械では効率良く解けない問題が存在することが示唆されたので，確率的アルゴリズムは強い Church-Turing の提唱に対する挑戦となった．この挑戦は強い Church-Turing の提唱を少し変形することで容易に解決したかにみえた．

> 如何なるアルゴリズムも確率的 Turing 機械で効率良くシミュレートできる．

強い Church-Turing の提唱におけるこのような**その場凌ぎ**の変更は読者に不快に映るかも知れない．後になってまた別の計算モデルが現れても，Turing 計算モデルの範疇では効率的に解けない問題が効率的に解けるようになるのではないか？如何なる他の計算モデルをも効率良くシミュレートできると保障されている計算モデルが１つでも見つかる途があるのではないか？

この疑問に触発されて 1985 年に David Deutsch は，物理学の法則を用いてもっと強い Church-Turing の提唱を**導く**ことはできないかと自問した．**その場凌ぎ**の仮説を採用する代わりに，物理学理論の位置づけと同様な確固とした基礎づけを Church-Turing の提唱に与えるために，Deutsch は物理学理論に着目した．Deutsch はとりわけ**任意の**物理システムを効率良くシミュレートできる計算デバイスを定義することを試みた．物理学法則は究極的に量子力学的であるので，Deutsch は必然的に量子力学原理に立脚した計算デバイスを考えることになった．このデバイスは 49 年前に Turing が定義した機械の量子版であり，ついに本書でいう量子コンピュータの概念に到達したのである．

本書の執筆時点で Deutsch の普遍的量子コンピュータ概念が，任意の物理システムを効率良くシミュレートするかどうかは明らかになっていない．この推論を証明するか拒否するかは，量子計算と量子情報分野の大きな問題の１つである．

例えば，量子場の理論の何かの効果や弦理論の難解な効果，量子重力や何か他の物理学理論が，Deutsch の普遍的量子コンピュータを超越してさらに一層強力な計算モデルに導くかも知れない．この段階で我々にはわからない．

Deutsch が量子コンピュータモデルを実現したのは，強い Church-Turing の提唱に対する挑戦であった．確率的 Turing 機械も含めて古典コンピュータが効率的解を持たない計算問題を量子コンピュータが効率的に解けるかどうかを Deutsch は自問した．実際に彼は古典コンピュータをしのぐ計算能力を量子コンピュータが持ち得ることを示唆する，簡単な例を構築したのである．

Deutsch により印されたこの目覚ましい第一歩は，次に続く 10 年間に多くの人々によって改良が加えられ，1994 年に Peter Shor が非常に重要な 2 つの問題 — 整数の素因数 (prime facor) を見つける問題と，いわゆる「離散対数」(discrete logarithm) 問題— が量子コンピュータで効率良く解けることを示した証明で頂点に達した．これら 2 つの問題は現在でもなお古典コンピュータでは効率的解がないと広く信じられているので，この成果は世間一般の関心を引きつけた．Shor の成果は量子コンピュータが Turing 機械より，さらに確率的 Turing 機械よりも強力であることを強く示すものである．量子コンピュータの能力を示す今ひとつの根拠が 1995 年に示された．Lov Grover はもう 1 つの重要な問題 — 構造を持たない探索空間における探索問題— の解が量子コンピュータで高速化できることを示した．Grover のアルゴリズムは Shor のアルゴリズムのような素晴らしい高速化をもたらすものではないが，探索に基礎を置く手法が広い用途を持つために，Grover のアルゴリズムにもかなりの関心が集まった．

Shor や Grover のアルゴリズムが発見されたのと時を同じくして，多くの人々が Richard Feynman が 1982 年に示唆したアイディアの実現をはかっていた．Feynman は，古典コンピュータで量子力学システムをシミュレートするには本質的困難がありそうなことを指摘し，量子力学原理に基づくコンピュータが構築できればこれらの困難が回避できるであろうと示唆した．1990 年代に幾つかの研究チームがこのアイディアの実現に努め，古典コンピュータで効率的シミュレーションが知られていないシステムを，実際に量子コンピュータが効率良くシミュレートできることを示した．将来の量子コンピュータの主要な用途の 1 つは，古典コンピュータでシミュレーションが困難であるが，科学的・工学的に深い意義を持つ問題である量子力学システムのシミュレーションになりそうである．

古典コンピュータに比べて量子コンピュータが素早く解けるその他の問題には何があるか？ 手短にいうと，答えはわからない．良い量子アルゴリズムが出現することは**難しそう**にみえる．悲観論者ならば量子コンピュータはすでに発見された応用以外には役に立たないからだと考えるかも知れない！ 我々の考えは少し違う．量子コンピュータのアルゴリズム設計が難しいのは，設計者が古典コンピュータのアルゴリズム構築に現れない2つの困難な問題に直面しているからである．1つは我々人間の直観は古典（物理学）的世界に根ざしている．もし我々がその直観をアルゴリズム構築の手助けに用いると，我々が見つけるアルゴリズムのアイディアは古典的アイディアとなる．良い量子アルゴリズムを設計するには，設計プロセスの少なくとも一部に対して，古典的直観から希望するアルゴリズムの目的を達成すべき真の量子効果に「切り替え」なければならない．2つ目は，アルゴリズムを本当に興味あるものにするには，単に量子力学的にするだけでは不十分である．そのアルゴリズムは如何なる現存の古典アルゴリズムに比べても**より良く**なければならない！ 同等の性能を有する古典アルゴリズムが存在するのでまだ広く関心を集めるには至っていないが，これができれば量子力学の本当の量子的特徴を利用したアルゴリズムが見いだせる可能性が生まれる．この2つの問題を抱えているので，新量子アルゴリズムの構築は将来に向けた挑戦課題である．

量子コンピュータ対古典コンピュータの能力比較をより広い観点から一般的に取り扱うことはできないか？ 古典コンピュータに比べて量子コンピュータが ― 実際に正しいとして ― 強力である理由は何か？ どのようなクラスの問題を量子コンピュータは効率良く解けるのか？ そのクラスは古典コンピュータで効率良く解ける問題とどのような関係にあるのか？ 量子計算と量子情報に関して最も興奮するのは，これらの問いに対する答えが如何に**少ししかわかっていない**かという点である！ これらの疑問をもっと理解することは将来に対する大きな挑戦である．

量子計算の最前線に来たので，量子計算と量子情報に貢献する別の一連の概念に話題を変える．それは情報理論である．1940年代にコンピュータ科学が発展したのと時を同じくして，**通信**に対する理解にも別の革命が起きつつあった．1948年にClaude Shannonは情報と通信の近代的理論の基礎を築いた有名な2つの論文を発表した．

Shannonが達成した重要なステップはおそらく**情報概念を数学的に定義**したことである．多くの数理科学において基本的定義にはかなりの柔軟性が許される．

次の疑問をしばらく素朴に考えてみよう．情報源の概念を数学的に定義するにはどうすればいいか？ この問題に関して幾つかの**異なる**答えが広く用いられてきた．しかし Shannon が到達した定義は最も実りある進歩した理解である点で抜きん出ており，実世界の通信に関する（すべてではないが）多くの問題を正確に反映して，奥深く実り多い成果と豊富な内容を持つ体系をもたらした．

Shannon は通信チャンネル上の情報通信に関連して2つの重要な疑問を抱いた．第1は通信チャンネルを通じて情報を送るにはどのようなリソースが必要か？ 例えば，電話会社は与えられた電話ケーブルを通じてどれほどの情報量が実際に送れるかを知る必要がある．第2に通信チャンネルの雑音に妨げられることなく情報を保護して送れるか？

Shannon は情報理論の2つの基本定理を証明することによりこれら2つの疑問に解答を与えた．最初の Shannon の**雑音のないチャンネルの符号化定理** (noiseless channnel coding theorem) は，情報源出力を蓄積するのに必要な物理的リソースを定量化するものである．Shannon の第2基本定理である**雑音のあるチャンネルの符号化定理** (noisy channnel coding theorem) は，雑音のある通信チャンネルを通じてどれだけ多くの情報を信頼性良く伝送できるかを定量的に示す．雑音があるときに高信頼性の伝送を行うために，Shannon は送る情報を保護する**誤り訂正符号** (error-correcting code) が使えることを示した．Shannon の雑音のあるチャンネルの符号化定理は誤り訂正符号でまかなえる保護の上限を示すものである．不幸にして Shannon の定理はこの限界を達成する実用的誤り訂正符号を明示的に示すものではない．Shannon の論文当時から現在に至るまで研究者達は Shannon の定理の限界に近づくことを目指して，多くのより良い誤り訂正符号を構築してきた．今では誤り訂正符号の高度な理論が存在し，ユーザが良い誤り訂正符号を設計するための豊富な選択肢を提供している．そのような符号は，例えばCD プレーヤ，コンピュータモデム，衛星通信システムなど多くの場所で使われている．

量子情報理論は同様の展開でこれに続いた．1995 年に Ben Schumacher は Shannon の雑音のない符号化定理の量子版を考え，実体のある物理的リソースとして「量子ビット」つまり「q ビット」を定義した．しかし，量子情報に対するは Shannon の雑音のあるチャンネルの符号化定理の量子版はまだ知られていない．それにもかかわらず古典的理論とのアナロジーで量子誤り訂正符号化理論が

構築されており，すでに述べたように雑音があっても量子コンピュータが効率良く計算でき，また雑音がある**量子**チャンネルを通じて通信ができることが示されている．

実際に量子誤り訂正符号を理解し発展させるうえで，誤り訂正の古典的概念は非常に重要である．1996 年に Robert Calderbank と Peter Shor，および Andrew Steane の 2 つの別のグループは重要な量子符号のクラスを発見した — 彼らの頭文字を取って CSS 符号と呼ばれている．この研究は Robert Calderbank，Eric Rains，Peter Shor，Neil Sloane のグループと Daniel Gottesman によってその後独立に発見された固定部分群符号 (stabilizer code) に含まれる．古典線形符号化理論の基本概念のうえに構築することによって，これらの発見は量子誤り訂正符号と量子計算と量子情報への応用の急速な理解を大いに促した．

量子誤り訂正符号は量子状態を雑音から保護するために考え出された．量子チャンネルを使って通常の**古典的**情報を送るとどうなるか？ そのときの効率はどうか？ この分野で幾つの驚くべき発見があった．1992 年に Charles Bennett と Stephen Wiesner は送信器から受信器に向けて **1 つの**量子ビットを送ることによって **2 つの**古典ビットの情報を送る方法 — **超高密度符号化** (superdense coding) — を示した．

もっと興味深いのは**分散量子計算** (distributed quantum computation) の成果である．ネットワーク化された 2 つのコンピュータが 1 つの問題を解く場合を考える．その問題を解くためにどれくらいの通信が必要となるか？ 最近示されたところによれば古典コンピュータのネットワークで必要な通信に比べて，量子コンピュータでは**指数関数的に少ない**通信で済ませられる．不幸なことに実際の状況下でこの問題が特に重要というわけではなく，幾つか望ましくない技術的制約を抱えている．分散古典計算に比べて分散量子計算が本質的に優位となる実世界の重要問題を見出すことは，将来の量子計算と量子情報への大きな挑戦である．

情報理論本来の話題に戻ろう．情報理論の研究は単一通信チャンネルの性質から始まる．その応用には単一通信チャンネルではなく多数のチャンネルよりなるネットワークを扱うことが多い．**ネットワーク情報理論** (networked information theory) は通信チャンネルのネットワークにおける情報伝送特性の問題を取り扱い，豊かで複雑な分野に発展している．

これに比べてネットワークの量子情報理論はまだほんの幼児期にある．非常に

基本的な疑問に関して，量子チャンネルネットワークの情報伝送能力について我々は少ししか知らない．最近数年幾つか印象的な予備的成果が得られているが，量子チャンネルに対する統一的なネットワーク情報理論はまだできていない．そのような一般理論ができればどんな価値があるかを納得してもらうには，ネットワーク量子情報理論の一例を示せば十分であろう．雑音のある量子チャンネルを通じて Alice から Bob に量子情報を送ると考える．もしチャンネル容量が量子情報に対して 0 であれば，Alice から Bob に**如何なる**情報も高信頼度で送ることは不可能である．それに代わって同期して働く 2 つのチャンネルのコピーを考える．直観的に明らかに（厳密にも証明できるが）このようなチャンネルも量子情報を送るには容量が 0 である．しかし，図 1.1 に示すようにもしも一方のチャンネルの方向を**反転**すれば，Alice から Bob に情報伝送するのに 0 でない容量が入手できることがある！ このような非直観的特質は量子情報の奇妙な性質の一端を示している．量子チャンネルネットワークの情報伝送性能をよりよく理解するのは量子計算と量子情報の重要な課題である．

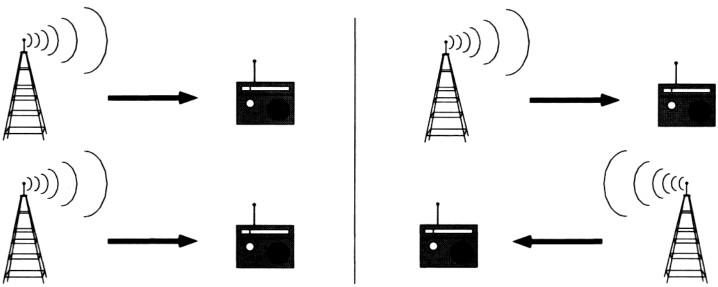


図 1.1: 古典的な雑音の多い 2 つのチャンネルが平行に設置されている場合，両方を組み合わせても情報伝送の容量は 0 である．驚くことではないが一方のチャンネルの方向を逆にしても情報伝送容量はやはり 0 である．量子力学的には伝送容量が 0 のチャンネルの一方の方向を逆転すると実際に情報が送れるようになる！

最後にもう一度別の分野に話題を変えて，古くからある注目すべき技術である**暗号** (cryptography) に話題を移そう．露骨に言えば，暗号は**互いに信用できないかもしれない** 2 人あるいはそれ以上の当事者間で**通信**または**計算**を行う問題である．よく知られている暗号問題は秘密メッセージの伝送である．例えば，できれば悪意ある第 3 者に傍受されることなく商品と引き替えにクレジットカード番号を商人に知らせたいとする．これを行うのが**暗号プロトコル**(cryptographic protocol)

である．後でこの暗号プロトコルが如何に役立つか詳しく述べるが，さしあたり二三簡単な特徴を述べるにとどめる．最も重要なのは**秘密鍵暗号システム** (private key cryptosystem) と**公開鍵暗号システム** (public key cryptosystem) の違いである．

秘密鍵暗号システムの働きは2人の当事者「Alice」と「Bob」が彼らだけしか知らない**秘密鍵** (private key) を共有することにより通信することである．この時点では鍵が正確にどのようなものであるかはあまり気にせず，とりあえず一連の0と1であると考える．重要なことはAliceがこの鍵を使ってBobに送ろうとする情報を**暗号化**することである．Aliceは暗号化した後暗号化情報をBobに送り，Bobは元の情報を復元しなければならない．Aliceの暗号化は厳密に**秘密鍵に依存**しており，それを復元するにはBobはAliceが行った操作を元に戻すために同じ秘密鍵を知っていなければならない．

不幸にして秘密鍵暗号システムは多くの場合幾つか厳しい問題点を抱えている．最も基本的問題は如何にして鍵を配送するか？である．多くの場合に鍵配送問題は秘密に通信をするという元の問題と同じくらい困難である — 悪意ある第三者が鍵配送を盗聴し傍受した鍵を使って伝送された暗号メッセージを復号するかも知れない．

初期の量子計算と量子情報における発見の1つに量子力学を用いてAliceとBobの安全性を傷つけることなく鍵を配送できるというものがある．この手順は**量子暗号** (quantum cryptography) または**量子鍵配送** (quantum key distribution) と呼ばれる．基本的アイディアは，一般に観測をすれば被観測システムに擾乱を与えるという量子力学原理を利用する．もしもAliceがBobに鍵を伝送しようとしているときに盗聴者が介入すれば，盗聴者の存在はAliceとBobが使っている通信チャンネルの擾乱として明瞭になる．そうすればAliceとBobは盗聴者が介入していたときに共有した鍵を放棄して，再度鍵配送を試みればよい．最初の量子暗号の概念は1960年代後半にStephen Wiesnerによって提案されたが，不幸なことにその論文は受理されなかった．1984年にCharles BennettとGilles BrassardはWiesner研究に則って，量子力学を用いてAliceとBobの間で安全性を損なうことなく鍵を配送できるプロトコルを提案した．それ以来多くの量子暗号プロトコルが提案され，プロトタイプ実験が行われた．本書執筆時点において実験プロトタイプは限られた範囲ではあるが，実世界の応用に使える段階に近

づきつつある．

第2の暗号系は**公開鍵暗号システム** (public key cryptosystem) である．公開鍵暗号システムでは Alice と Bob が前もって秘密鍵を共有しておく必要がない．実際に Bob は単に**一般に入手できる**「公開鍵」を発行する．Alice はこの公開鍵を使ってメッセージを暗号化して Bob に送る．興味があるのは，第三者は Bob が発行した公開鍵でメッセージを**復号化できない**ことである！ 厳密に言えば**できない**というべきではない．むしろ暗号化変換が非常に巧妙かつ類を見ない方法で行われるので，公開鍵だけの知識では復号化が（不可能ではないが）**極めて難しい**．復号化を簡単に行うために Bob は公開鍵に整合した**秘密鍵**を持っており，これを使って彼は**容易**に復号化を行うことができる．この秘密鍵は Bob 以外の誰にも知らされておらず，したがって誰も他に公開鍵だけから秘密鍵を得るほどの計算能力を持っていそうにないという範囲内で，Bob は自分だけが Alice のメッセージ内容を読むことができると確信できる．公開鍵暗号システムは通信に先立って Alice と Bob が秘密鍵共有の必要をなくして鍵配送問題を解決する．

驚くべきことに公開鍵暗号は 1970 年代半ばまで広く使われることはなかった．この頃になって Whitfield Diffie と Martin Hellman，および Ralph Merkle が独立に提案して暗号分野に革命をもたらした．少し後になって Ronald Rivest，Adi Shamir および Leonard Adleman が **RSA 暗号システム** (RSA cryptosystem) を開発した．この暗号は本書執筆時点では最も広く実用展開されている公開鍵暗号システムであり，安全性と実用性を見事にバランスさせたシステムであると信じられている．1997 年にこれらのアイディア — 公開鍵暗号，Diffie-Hellman と RSA 暗号システム — は英国情報局 GCHQ の研究者達によって 1960 年代および 1970 年代初期に発明されたことが明らかにされた．

公開鍵暗号システムにおける安全性の鍵は，公開鍵しかなければ暗号化段階の逆を行うのが困難であるところにある．例えば，RSA の暗号化の逆を行うのは素因数分解と密接に関連した問題である．RSA で想定されている安全性の多くは素因数分解が古典コンピュータで解決困難な問題だという確信からきている．しかし，量子コンピュータにおける素因数分解の Shor の最初のアルゴリズムを用いれば RSA を破ることができる．同様に — 離散対数に対する Shor の量子アルゴリズムのような — 離散対数問題を早く解くアルゴリズムができれば他の公開鍵暗号システムも破ることができる．暗号符号を打ち破る量子コンピュータの実際

的応用が量子計算と量子情報への多くの興味を喚起した．

我々は量子計算と量子情報の歴史的源流について見てきた．もちろんこの分野が成長し成熟するにつれて量子計算と量子情報を源として新規の関連分野が登場してきた．

これらの中で最も顕著なものは**量子もつれ** (量子絡み合い，quantum entanglement) の研究であろう．もつれは量子力学に特有の**リソース** (資源，resource) であり，量子計算と量子情報の多くの最も興味ある応用において重要な役割を演ずるものである．もつれはいわば大昔の青銅器時代に対する鉄器のような存在である．近年もつれは — エネルギー，情報，エントロピー，その他基礎資源と比肩する重要さを持つ — 自然界の基本的資源であると考えられ，その性質のより良い理解を目指して膨大な努力が払われている．今のところまだもつれに関する完全な理論は確立していないが，この量子力学の奇妙な性質に関する理解は進んでいる．もつれの性質をさらに研究することにより，量子計算と量子情報に新たな応用の展開をもたらす洞察が生まれるのを多くの研究者が望んでいる．

1.1.2　将来の方向

量子計算と量子情報の歴史と現状について見てきた．将来はどうであろうか？ 量子計算と量子情報は科学に，技術に，そして人類に何をもたらすか？ 量子計算と量子情報はその母体であるコンピュータ科学，情報理論，そして物理学に何をお返しできるか？ 量子計算と量子情報の鍵となる問題は何か？ 詳細な研究に移るまえに，これら包括的な疑問に対して手短に意見を述べておく．

量子計算と量子情報によって我々は**計算を物理的に考える**ことを学び，このアプローチが情報処理と通信に対する，多くの新たな刺激的可能性を生み出すことを見出してきた．コンピュータ科学者と情報理論家には新しい豊かな探索の方法論がプレゼントされた．実際のところ広い意味で量子力学に限らず**如何なる理論物理学**でも情報処理と通信理論の基礎となり得ることを学んだ．これらの探索の果実は何時の日にか，今日の計算や通信システムを遙かに越えた能力を持つ情報処理デバイスとなって実を結び，それに伴って社会全体に利益と新たな課題を同時にもたらすであろう．

量子計算と量子情報は確かに物理学者に多くの挑戦課題をもたらすが，長期的

に物理学に何をもたらすかについては少し微妙なところである．計算を物理的に考えることを学んだように，**物理学を計算理論的に考える**ことも学ぶことができる．伝統的に物理学は「要素」物体や単純なシステムを理解することに焦点を絞った学問分野であった一方で，「自然」にはより大きくより複雑になるときに初めて現れる多くの興味ある側面が存在する．化学と工学はある程度そのような複雑さを扱うが，たいていの場合むしろ**その場限り**のやり方であることが多い．量子計算と量子情報からの１つのメッセージは，微小なものと比較的複雑なものの間に横たわる隔絶を越えるための，新たなツールが得られるということである．つまり計算とアルゴリズムは，そのようなシステムを構成し理解する系統的手法を提供する．これらの分野からの概念は物理学に新たな見識をもたらし始めている．我々の希望は今後これらの夢が花開き，物理学の全側面に実り多い理解がもたらされることである．

量子計算と量子情報の下に横たわる，幾つかの重要な動機とアイディアについて手短に調べてきた．１章の残りの節では現状分野の鳥瞰図を示すためにこれら動機とアイディアについて，より技術的ではあるがわかりやすく紹介する．

1.2 量子ビット

ビット(bit) は古典計算と古典情報の基本概念である．量子計算と量子情報は類似の概念である**量子ビット** (quantum bit)，あるいは略して **q ビット** (qubit) のうえに構築される．本節では単一および多 q ビットの性質を紹介し古典ビットと比較対照する．[1]

q ビットとは何か？ 我々は q ビットをある特定の性質を持つ**数学的対象**として記述していく．読者は「ちょっと待ってほしい．q ビットは物理的対象だと思っていた」というかも知れない．確かにビットと同様に q ビットは現実的物理システムとして実現されており，1.5 節と 7 章で抽象的数学の観点と実際のシステムとが如何に関係しているかを詳しく述べる．しかしたいていの場合に我々は q ビットを抽象的な数学的対象として扱う．抽象的対象として q ビットを扱う美しさとは，実現するための特定のシステムに依存することなく，量子計算と量子情報の

[1]訳注： 以下英語版において “quantum bit” に代わって “qubit” が用いられるのに対応して，日本語版でも「量子ビット」に代えて「q ビット」を使用する．

一般理論を組み立てる自由度が与えられることである．

しからばqビットとは何か？ 古典ビットに**状態**— 1あるいは0 — があるように，qビットも状態を持つ．qビットの2つの可能な状態は状態 $|0\rangle$ と $|1\rangle$ であり，古典ビットの状態0と1に対応すると考えてもかまわない．$|\ \rangle$ の記号は**Diracの記号** (Dirac notation) と呼び，量子力学の状態を表す標準的記号なのでこれから頻繁に目にすることになる．ビットとqビットの違いはqビットが $|0\rangle$ または $|1\rangle$ **以外**の状態も取り得ることである．つまり，状態の**線形結合**を形作ることが可能でありしばしば**重ね合せ** (superposition) と呼ぶ．

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{1.1}$$

数 α および β は複素数であるが，多くの場合に実数と考えても失うものは多くない．換言すればqビット状態は2次元複素ベクトル空間のベクトルである．特定の状態 $|0\rangle$ と $|1\rangle$ を**計算基底状態** (computational basis state) と呼び，このベクトル空間の正規直交基底を構成する．

我々はビットを調べてそれが0，1のいずれの状態にあるかを決めることができる．例えば，コンピュータがメモリの内容を取り出すときにいつもこれを行っている．驚くことに我々はqビットを調べてその量子状態，つまり α と β の値，を決めることはできない．量子力学の教えるところでは，その代わりに我々が得ることができるのは量子状態に関してもっと制約された情報だけである．qビットを測定するときに我々が得る結果は確率 $|\alpha|^2$ で結果が0，または確率 $|\beta|^2$ で結果が1である．全確率の和は1なので当然 $|\alpha|^2 + |\beta|^2 = 1$ である．幾何学的解釈ではこれはqビット状態が長さ1に正規化される条件である．したがって一般にqビット状態は2次元複素ベクトル空間の単位ベクトルを表す．

観測できないqビット状態と我々が行う観測という対立する2つの概念は，量子計算と量子情報の中心をなすものである．世界の多くの抽象的モデルでは，ちょうど建築家の設計図が最終的な建物に対応するように，抽象的要素と実世界の間に直接の対応関係が存在する．このような直接の対応が量子力学にないので，量子システムの振る舞いを直観的に考えることが困難になる．しかし間接的対応関係ならば存在しており，状態の性質が異なればそれに応じて別の測定結果を与えるように，qビット状態を操作し変換することができる．このようにしてこれら量子状態は実験的に証明できる現実の結果を与え，これが量子計算と量子情報に

とって本質的能力となることをこれから見ていく．

qビットが重ね合せ状態を取り得ることは，我々の回りの物理的世界における「常識」的理解に反する．古典ビットは表か裏が出るコインのようなものである．不完全なコインならばコインの端で立ってバランスするような中間的状態もあるかも知れないが，理想的場合ではこれは無視できる．これに対してqビットは — 観測されるまでは — $|0\rangle$ と $|1\rangle$ の間の**連続した状態** (continuum) に存在し得る．ここでもう一度強調しておくが，qビットが一度測定されるとその測定結果として — 確率的に — 「0」か「1」だけを与える．例えば，qビットは状態：

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \tag{1.2}$$

を取ることができる．これを測定すると 50 %（$= |1/\sqrt{2}|^2$）の時間は結果 0，50 %の時間は結果 1 を与える．式 (1.2) の状態を $|+\rangle$ と表して今後しばしば使用する．

このように奇妙な性質をもつにもかかわらずqビットは確実に現実のものであって，その存在と振る舞いは広範囲に実験で確認されており（1.5 節と 7 章（第 II 巻）で議論する），多くの異なる物理的システムによってqビットが実現されている．如何にしてqビットが実現できるかを具体的に実感するには，その幾つかの実現法を列挙するのがよいであろう．光子の 2 つの異なる偏光，一様磁界中の核スピンの配列，図 1.2 に示すような単一原子における電子軌道の 2 つの状態等がある．原子モデルで電子はいわゆる「基底」状態 (ground state) または「励起」状態 (excited state) に存在しそれぞれを $|0\rangle$，$|1\rangle$ と呼ぶ．原子に適切なエネルギーの光を適切な時間照射すると電子を $|0\rangle$ 状態から $|1\rangle$ 状態に，あるいはその逆に動かすことができる．もっと興味深いのは光を照射する時間を短くすると，最初 $|0\rangle$ 状態にいた電子を $|0\rangle$ と $|1\rangle$ の「途中」の状態，すなわち $|+\rangle$ 状態にすることができる．

当然ながら重ね合せ状態に与える「意味」ないし「解釈」と，本来確率的な性質を持つ量子システムの観測について多大の注意が払われてきた．しかし，本書では全般的にその種の議論に立ち入らないことにする．その代わりに我々は予測可能な数学上および概念上の描像を作ることを目指す．

次のような幾何学的表現がqビットを考えるうえで有用な描像である．$|\alpha|^2 + |\beta|^2 = 1$ であるので，式 (1.1) を次のように書き換える．

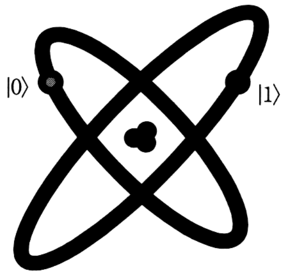


図 1.2: 原子の 2 つの電子準位で表した q ビット．

$$|\psi\rangle = e^{i\gamma}\left(\cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\right) \tag{1.3}$$

ここで，θ, φ および γ は実数である．2 章で右辺最初の因子 $e^{i\gamma}$ は観測可能な効果をもたらさないので無視できることがわかる．そこで実効的に次のように書ける．

$$|\psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle. \tag{1.4}$$

図 1.3 に示すように θ と φ は 3 次元単位球面上の点を定義する．この球面をしばしば **Bloch 球** (Bloch sphere) と呼ぶ．これは単一 q ビット状態を視覚化する便利な方法であり量子計算と量子情報に関する概念の優れたテストベッドとして使う．本章で述べる単一 q ビットの多くの操作は Bloch 球上の描像で記述できる．しかし Bloch 球は多 q ビットに対して簡単に一般化できないので，この直観は制約を受けることを心に留めておかねばならない．

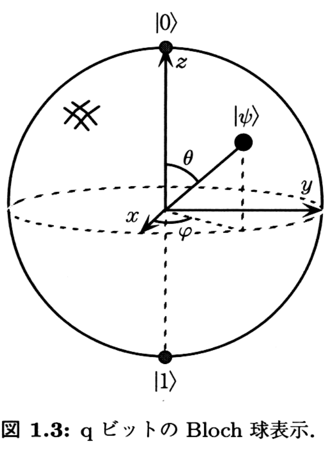


図 1.3: q ビットの Bloch 球表示．

q ビットによってどれくらい多くの情報が表現できるか？ 逆説的に言えば単位球面上に無限に多くの点があるので，原理上 θ を 2 進数変換で無限に展開をすればシェークスピアのすべての著作でも収めることができる．しかし，観測時の q ビットの振る舞いを考慮するとこの結論は誤解を招く．q ビットを測定すると 0 または 1 のみを与えることを思い出そう．さらに測定によって q ビット状態は**変化**し，$|0\rangle$ と $|1\rangle$ の重ね合せ状態から測定結果に対応した特定の状態に収縮 (collapse) する．例えば，$|+\rangle$ 状態を測定した結果が 0 であれば測定後の q ビットの状態は $|0\rangle$ となる．なぜこのような収縮が起きるのか？ 誰も知らない．2 章で述べるように，この振る舞いは単に量子力学の**基本公理** (fundamental postulate) の 1 つなのである．我々の目的との関連でいえば 1 回の測定で q ビット状態について 1 ビットの情報しか得られないので，見かけ上の逆説は解決される．無限に多くの同等の q ビットを測定すると式 (1.1) で与えられる q ビット状態の α と β を決定することができる．

もっと興味あるのは次の疑問である．**もしも測定しなければ** q ビットでどれだけの情報を表現できるか？ 測定できなければ情報の定量化のしようがないので，これはまやかしの質問である．にもかかわらず自然は q ビットのように閉じられた量子システムが「測定」されることなく時間発展するときには，状態を記述する連続変数 — α や β — が変化しないので，ここにはある種の重要な概念が含まれる．ある意味で q ビット状態の中に自然は多くの「隠れた情報」(hidden information) を隠し持っている．もっと興味深いことにこの付加的な「情報」の潜在的量は q ビットの数が増えると，それに伴って指数関数的に増加することがまもなく明らかになる．この**隠れた量子情報** (hidden quantum information) を理解することが本書の多くで取り組む疑問であり，量子力学を情報処理の強力なツールにしている根底に潜む疑問でもある．

1.2.1　多 q ビット

Hilbert 空間は大きな空間である．— Carlton Caves

2 個の q ビットがあるとする．これが古典ビットならば 4 つの取り得る状態 00, 01, 10 および 11 がある．これに対応して 2 個の q ビットシステムには $|00\rangle$, $|01\rangle$,

$|10\rangle$, $|11\rangle$ で表される**計算基底状態** (computational basis state) がある．q ビット対もこれら 4 つの重ね合せ状態にあるので，2 個の q ビットの量子状態は各計算基底状態に関する複素係数 — **振幅** (amplitude) とも呼ぶ — を含んでいる．2 個の q ビットを記述する状態ベクトルは

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle. \tag{1.5}$$

で与えられる．単一 q ビットの場合と同様に，測定結果 x $(= 00,\ 01,\ 10$ または $11)$ は確率 $|\alpha_x|^2$ で生じ，測定後の q ビット状態は $|x\rangle$ となる．確率の合計が 1 になる条件は正規化条件 $\sum_{x\in\{0,1\}^2} |\alpha_x|^2 = 1$ で表される．ここで，記号「$\{0,1\}^2$」は「各文字が 0 または 1 であり，長さ 2 の記号列の集合」を意味する．2 個の q ビットシステムに対して，その部分集合だけ — 例えば最初の q ビットだけ — でも測定できる．その働きはおそらく推測できるように，最初の q ビットのみが 0 である結果の確率が $|\alpha_{00}|^2 + |\alpha_{01}|^2$ で，測定後の状態が

$$|\psi'\rangle = \frac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}. \tag{1.6}$$

で与えられる．測定後の状態も合理的な量子状態として期待される正規化条件を満たすように，因子 $\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}$ で再正規化していることに注意する．

Bell 状態 (Bell state) もしくは **EPR 対** (EPR pair) と呼ぶ 2 個の q ビット状態は重要である．

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{1.7}$$

この一見何の変哲もない状態が量子計算と量子情報において多くの驚きをもたらす．これが 1.3.7 項と 2.3 節でそれぞれ取り扱う量子テレポーテーションや超高密度符号化の鍵となる構成要素であり，その他多くの興味ある量子状態の原型となるものである． Bell 状態は次のような性質を持っている．最初の q ビットを測定すると 2 つの可能な結果を得る．1 つは確率 1/2 で 0，測定後の状態は $|\varphi'\rangle = |00\rangle$，もう 1 つは確率 1/2 で 1，測定後の状態は $|\varphi'\rangle = |11\rangle$ である．その結果，第 2 の q ビットを測定すると常に最初の q ビットと同じ結果を与える．つまり測定結果が**相関** (correlate) を有している． 実際最初に Bell 状態の第 1 または第 2 の q ビットに何かの演算を行ってから，次に他のタイプの測定を行うことができて，そのときにも最初と 2 番目の q ビットの測定結果にこの興味ある相関が存在する

ことがわかる．この相関は — 最初に Bell 状態のような状態の奇妙な性質を指摘した — Einstein，Podolsky，Rosen の有名な論文以来強い関心の的となってきた．EPR の洞察を John Bell が取り上げて議論を進め，測定における Bell 状態の相関は**古典的システム間に存在する如何なる相関より強い**ことを示した．この結果は 2.6 節で詳しく述べるが，これは古典的世界の可能性を越える情報処理を量子力学で行えることを最初に暗示したものといえる．

我々は一般に n 個の q ビットを考えることができる．このシステムの計算基底状態は $|x_1x_2\ldots x_n\rangle$ の形をしており，このシステムの量子状態は 2^n 個の振幅で規定される．$n=500$ とすると，この数は宇宙に存在すると推定される原子の数より大きくなる！ この数の複素数をすべて蓄積することは，考えられる限りの古典コンピュータでは不可能であろう．Hilbert 空間は実に大きな空間なのである．しかし自然は数百の原子しか含まないシステムに対してですら原理上このように膨大な量のデータを取り扱っているのである．これはあたかも自然が 2^{500} 枚の隠れた計算用紙を脇に置いて，システムの時間発展に合わせて計算をしているようなものである．この膨大な潜在的計算能力が我々が大いに利用したいと望んでいるものである．しかし如何にすれば量子力学を計算として考えることができるのであろうか？

1.3　量子計算

量子状態に生じている変化は**量子計算** (quantum computation) の言語で記述できる．古典コンピュータが配線と論理ゲートからなる電気回路で作られているのと同様に，量子コンピュータは量子情報を運び操作するための配線と基本的**量子ゲート** (quantum gate) よりなる**量子回路** (quantum circuit) によって作られる．本節では幾つかの簡単な量子ゲートについて述べ，二三の回路例を示して q ビットのテレポーテーションを含む応用について述べる．

1.3.1　単一 q ビットゲート

古典コンピュータ回路は配線と**論理ゲート** (logic gate) により構成される．配線は回路中の情報を運び，論理ゲートは情報を変換して操作する．例えば，古典

的単一ビット論理ゲートを考える．このクラスで意味があるのは NOT ゲートであり，その働きは**真理値表** (truth table) で定義され，$0 \to 1$ および $1 \to 0$ — つまり状態 0 と 1 の入れ替え — が行われる．

類似の量子 NOT ゲートが q ビットに対して定義できるであろうか？ 状態 $|0\rangle$ が状態 $|1\rangle$ に，そしてその逆に変化するプロセスがあると想像する．そのようなプロセスは明らかに NOT ゲートの量子版として打ってつけの候補になる．しかし量子ゲートのさらに詳しい性質がわからなければ，状態 $|0\rangle$ と $|1\rangle$ に対するゲートの作用を示すだけでは，$|0\rangle$ と $|1\rangle$ の重ね合せ状態に対してはどうなるかわからない．実際には量子 NOT ゲートは線形に働くので，状態

$$\alpha|0\rangle + \beta|1\rangle \tag{1.8}$$

を $|0\rangle$ と $|1\rangle$ が入れ替わった状態

$$\alpha|1\rangle + \beta|0\rangle \tag{1.9}$$

に変化させる．なぜ量子 NOT ゲートが線形に働き何か他の非線形な働きをしないのかは，興味ある問題であるがその答えは皆目わからない．この線形の振る舞いは量子力学に一般的な性質であり，経験的にも根拠のあることである．これにとどまらず非線形な動作があると，タイムトラベルや光速より速い通信，熱力学第 2 法則の破綻というような明らかな矛盾が生じる．この点について後の章で詳しく調べるが，取りあえず与えられたものとして扱う．

量子ゲートの線形性から直接導かれることの 1 つに，量子 NOT ゲートを行列の形で表す便利な方法がある．行列 X が次に示すように量子 NOT ゲートを表すと定義する．

$$X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{1.10}$$

(量子 NOT ゲートを X で表すのは歴史的理由による.) 量子状態 $\alpha|0\rangle + \beta|1\rangle$ をベクトル表記で次のように書く：

$$\begin{bmatrix} \alpha \\ \beta \end{bmatrix}, \tag{1.11}$$

ここで上の要素は $|0\rangle$ に対する振幅，下の要素は $|1\rangle$ に対する振幅に相当する．量

子 NOT ゲートの出力は

$$X\begin{bmatrix}\alpha\\ \beta\end{bmatrix}=\begin{bmatrix}\beta\\ \alpha\end{bmatrix}. \tag{1.12}$$

で与えられる．NOT ゲートの作用は状態 $|0\rangle$ を取り上げて行列 X の最初の列に相当する状態で置き換え，同様に $|1\rangle$ を行列 X の第 2 の列に相当する状態で置き換えることである．

単一 q ビットに作用する量子ゲートは 2×2 の行列で記述できる．量子ゲートに用いられる行列には何か特別の制約があるか？ 確かにあることがわかっている．量子状態 $\alpha|0\rangle+\beta|1\rangle$ に対して正規化条件 $|\alpha|^2+|\beta|^2=1$ が必要であることを思い出そう．これはゲート作用後の量子状態 $|\psi'\rangle=\alpha'|0\rangle+\beta'|1\rangle$ に対しても成立しなければならない．量子ゲートを表す行列に対する条件は，単一 q ビットゲートを記述する行列 U が**ユニタリー** (unitary)，つまり $U^\dagger U=I$ であることである．ここで $U^\dagger$ は U の**転置共役**（随伴，adjoint）（U の行と列を転置して複素共役をとる），I は 2×2 の単位行列である．例えば，量子 NOT ゲートに対して $X^\dagger X=I$ は容易に証明できる．

驚くべきことにこのユニタリー性は量子ゲートに対する唯一の制約である．如何なるユニタリー行列でも妥当な量子ゲートを表す！ 意味のある単一ビットゲートはただ 1 つ — NOT ゲート — しかなかった古典的な場合と違って，単一 q ビットでは多くの重要な量子ゲートが存在する．後でよく使う 2 つのゲートをあげておく．Z ゲート：

$$Z\equiv\begin{bmatrix}1&0\\ 0&-1\end{bmatrix}, \tag{1.13}$$

は $|0\rangle$ を不変に保って，$|1\rangle$ の符号を変えて $-|1\rangle$ とする．Hadamard ゲート：

$$H\equiv\frac{1}{\sqrt{2}}\begin{bmatrix}1&1\\ 1&-1\end{bmatrix}. \tag{1.14}$$

このゲートは「NOT ゲートの平方根」であるかのように記述され，$|0\rangle$ を $|0\rangle$ と $|1\rangle$ の中間である $(|0\rangle+|1\rangle)/\sqrt{2}$（$H$ の第 1 列）に変換し，$|1\rangle$ をこれも $|0\rangle$ と $|1\rangle$ の中間である $(|0\rangle-|1\rangle)/\sqrt{2}$（$H$ の第 2 列）に変換する．しかし，簡単な代数計算でわかるように $H^2=I$ なので H^2 は NOT ゲートではなく，H を 2 回作用させると状態は変化しない．

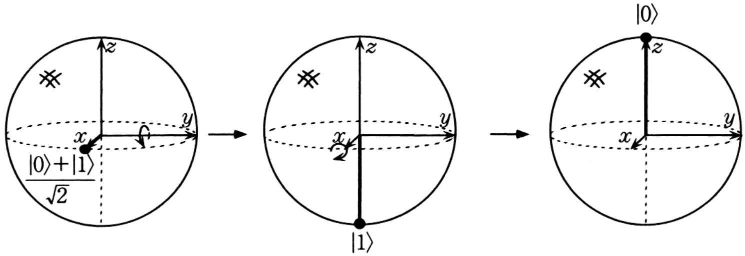


図 1.4: Bloch 球上での Hadamard ゲートの表現．入力状態 $(|0\rangle+|1\rangle)/\sqrt{2}$ に作用している．

Hadamard ゲートは最も有用な量子ゲートの 1 つであり，Bloch 球上でその作用を視覚化しておく価値がある．この描像において単一 q ビットゲートは球上での回転や反転に対応することがわかる．Hadamard 変換は図 1.4 に示すように $\hat{y}$ 軸の回りに 90° 回転し，次いで $\hat{x}$ 軸の回りに 180° 回転する．幾つかの重要な単一 q ビットゲートを図 1.5 に示し，古典的な場合と対照する．

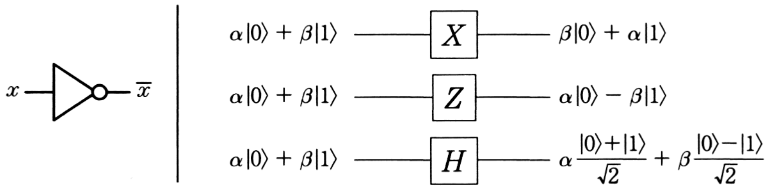


図 1.5: 単一ビット（左）と単一 q ビット（右）の論理ゲート．$\bar{x}$ は x の否定を表す．

2 × 2 のユニタリー行列は無限に多く存在し，したがって単一 q ビットゲートも無限に多い．しかし，完全に網羅した集合の性質は少数の集合の性質を調べれば理解できる．例えば，コラム 1.1 で説明するように任意の単一 q ビットのユニタリーゲートは回転：

$$\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}, \tag{1.15}$$

と，後で $\hat{z}$ 軸の回りの回転であることがわかるゲート：

$$\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}, \tag{1.16}$$

との積に分解できる．正確にはこの積に**グローバル位相シフト**(global phase shift) — $e^{i\alpha}$ の形をした一定値の乗数 — が掛けられる．これらのゲートはさらに分解できる．つまり，我々は任意の α，β，γ に対してこれらのゲートを実現する必要はなく，幾つかの特定の**固定値** α，β，γ のみを使って，これらのゲートを任意の精度で近似するゲートを作ることができる．このように**有限数**の量子ゲートを用いて，任意の量子 q ビットゲートを構築できる．一般的に如何なる数の q ビットに作用する任意の量子計算でも，量子計算に**普遍的**な有限数のゲート集合で生成することができる．そのような普遍的集合を手に入れるためにまず多 q ビットを対象とする幾つかの量子ゲートを導入する必要がある．

コラム 1.1: 単一 q ビット演算の分解

4.2 節（第 II 巻）で任意の 2×2 ユニタリー行列が次のように分解できることを示す．

$$U = e^{i\alpha}\begin{bmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{bmatrix}\begin{bmatrix} \cos\frac{\gamma}{2} & -\sin\frac{\gamma}{2} \\ \sin\frac{\gamma}{2} & \cos\frac{\gamma}{2} \end{bmatrix}\begin{bmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{bmatrix}, \tag{1.17}$$

ここで α，β，γ，δ は実数である．右辺第 2 の行列は通常の回転である．第 1 と第 3 の行列も異なる平面での回転を表すことがわかる．この分解を用いて**任意の**単一 q ビット量子論理ゲートの性能を規定できる．

1.3.2 多 q ビットゲート

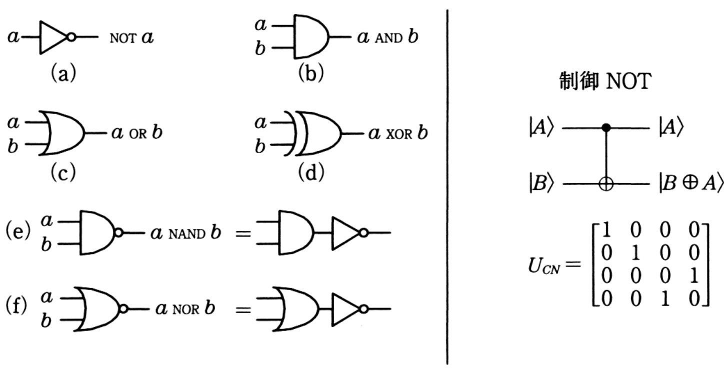
単一 q ビットから多 q ビットに一般化しよう．図 1.6 に注目すべき 5 つの多重ビットの古典ゲート AND，OR，XOR(exclusive-OR)，および NOR ゲートを示す．重要な理論的結論はビットに作用する如何なる関数も NAND ゲートだけで構成される回路で計算できるという重要な理論的結論があるので，NAND ゲートを**普遍的ゲート** (universal gate) と呼ぶ．これに対して XOR 単独，あるいは NOT と組み合わせても普遍的にはならない．これを検証する 1 つの方法は XOR ゲートを適用してもビット全体のパリティが変化しないことを見ればよい．その結果，NOT と XOR ゲートのみを含む如何なる回路も，もし 2 入力 x と y が同

じパリティならば出力も同じパリティとなり，計算できる関数のクラスが制約されて普遍性が損なわれる．

多 q ビット量子ゲートの原型は**制御 NOT ゲート**(controlled-NOT gate，略して CNOT gate) である．このゲートは 2 つの入力 q ビット — **制御 q ビット**(control qubit) と**標的 q ビット**(target qubit) — を有する．制御 NOT に対する回路表示を図 1.6 の右上に示す．上の線が制御 q ビット，下の線が標的 q ビットを表す．このゲートは次のような働きをする．もし制御 q ビットが 0 ならば標的 q ビットはそのままで，制御 q ビットが 1 ならば標的 q ビットは変化する．式で表すと，

$$|00\rangle \to |00\rangle;\ |01\rangle \to |01\rangle;\ |10\rangle \to |11\rangle;\ |11\rangle \to |10\rangle. \tag{1.18}$$

制御 NOT を記述するもう 1 つの方法は古典的 XOR ゲートの一般化と同じである．ゲートの作用は $|A, B\rangle \to |A, B \oplus A\rangle$，ここで $\oplus$ は 2 を法とする和を表す．これは XOR ゲートとまったく同じで制御 q ビットと標的 q ビットの XOR をとり標的 q ビットに記憶する．



$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

図 1.6: 左側は標準的な単一および多ビットゲート，右側は多 q ビットゲートの原型である制御 NOT ゲート．制御 NOT U_{CN} の行列表現は状態 $|00\rangle$，$|01\rangle$，$|10\rangle$，$|11\rangle$ の順に対応する振幅に対して書かれている．

制御 NOT の作用を記述するさらにもう 1 つ別の方法は行列表示であり，図 1.6 の右下に示している．U_{CN} の第 1 列が $|00\rangle$ に対する変換，そして同様に順次他の計算基底状態 $|01\rangle$，$|10\rangle$，$|11\rangle$ に対する変換を表すことが容易に証明できる．単一 q ビットの場合と同様に確率保存の条件は，U_{CN} が**ユニタリー行列** (unitary

matrix) つまり $U_{CN}^{\dagger}U_{CN}=I$ で表される．

制御 NOT ゲートは一種の一般化された XOR ゲートと見なせることを述べた．量子 NOT ゲートが古典 NOT ゲートを表すのと同じ意味で，NAND や普通の XOR ゲートのような他の古典ゲートもユニタリーゲートであると理解してもよいか？ これは良くないことがわかっている．その理由は，XOR や NAND ゲートは本質的に**非可逆**(irreversible) つまり**反転できない**(non-invertible) からである．例えば，XOR ゲートの出力 $A\oplus B$ が与えられたとしても，何が入力 A，B であったかを決めることはできない．XOR ゲートの非可逆的作用に伴って，回復できない**情報の損失**が生じたのである．一方，ユニタリー行列の逆行列もユニタリーなのでユニタリーな量子ゲートは常に反転可能であり，したがって量子ゲートは他の量子ゲートによって常に反転できる．この**可逆**(reversible) または**反転可能**(invertible) という意味で古典論理の作用を理解することは，量子力学の能力を計算に役立てるかどうかを理解する重要なステップである．可逆計算の方法に関する基本概念は 1.4.1 項で説明する．

当然制御 NOT 以外にも多くの興味ある量子力学ゲートが存在する．しかしある意味で制御 NOT と単一 q ビットゲートは他の全ゲートの原型である．その理由は次の注目すべき**普遍性**(universality) にある：**如何なる多 q ビット論理ゲートでも制御 NOT と単一 q ビットゲートで構成できる**．この証明は 4.5 節（第 II 巻）で行うが，これは古典 NAND ゲートの普遍性に相当する量子版である．

1.3.3 計算基底以外の基底による測定

状態 $\alpha|0\rangle+\beta|1\rangle$ における単一 q ビット測定により，確率 $|\alpha|^2$ または $|\beta|^2$ で結果 0 または 1 が得られ，q ビットがそれぞれ $|0\rangle$，$|1\rangle$ の状態に収縮することを述べた．実際に量子力学では確かに 1 回の測定で α と β を同時に取り出すことこそできないが，もう少し多様な測定が可能である．

状態 $|0\rangle$ と $|1\rangle$ は q ビットの基底状態として多くの可能な選択の 1 つにすぎない．もう 1 つの可能な選択は $|+\rangle\equiv(|0\rangle+|1\rangle)/\sqrt{2}$ と $|-\rangle\equiv(|0\rangle-|1\rangle)/\sqrt{2}$ の集

合である．任意の状態 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ を状態 $|+\rangle$, $|-\rangle$ を使って書き直すと

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \alpha\frac{|+\rangle + |-\rangle}{\sqrt{2}} + \beta\frac{|+\rangle - |-\rangle}{\sqrt{2}} = \frac{\alpha+\beta}{\sqrt{2}}|+\rangle + \frac{\alpha-\beta}{\sqrt{2}}|-\rangle. \tag{1.19}$$

状態 $|+\rangle$ と $|-\rangle$ をあたかも計算基底状態として扱って，この新しい基底に関して測定できることがわかる．当然基底 $|+\rangle$, $|-\rangle$ に関して測定を行えば，確率 $|\alpha+\beta|^2/2$ で結果「+」，確率 $|\alpha-\beta|^2/2$ で結果「−」が得られ，測定後の状態はそれぞれ $|+\rangle$ と $|-\rangle$ に収縮する．

一般に q ビットについて基底状態 $|a\rangle$ と $|b\rangle$ が与えられると，任意の状態をこれらの状態の線形結合 $\alpha|a\rangle + \beta|b\rangle$ で表現できる．さらにこれらの基底状態が**正規直交系**ならば**基底 $|a\rangle$，$|b\rangle$ に関して測定する**ことができ，確率 $|\alpha|^2$ で結果 a，確率 $|\beta|^2$ で結果 b を与える．確率に対して予想されるように $|\alpha|^2 + |\beta|^2 = 1$ となるために正規直交性の制約は必要である．同様に多 q ビットシステムを任意の正規直交基底に関して測定することが原理上可能である．しかし，測定が原理上可能であってもそれが容易にできるとは限らない．任意の基底に関して効率的測定ができるかという疑問には後で立ち返って議論する．

この拡大された量子測定形式を用いるには多くの理由があるが，結局のところ最も良い理由はこれである：その形式により観測した実験結果を記述できることである — その良い例が 1.5.1 項における Stern-Gerlach 実験の議論に出てくる．量子測定を記述する複雑で便利な（しかし本質的に同等な）形式を次章 2.2.3 項で述べる．

1.3.4　量子回路

我々はすでに二三の簡単な量子回路を目にしている．量子回路の要素をもう少し詳しく見てみよう．3 つの量子ゲートを含む簡単な量子回路を図 1.7 に示す．回路は左から右に向けて読む．回路の各線は量子回路の 1 本の**配線** (wire) を表す．この配線は必ずしも物理的な線に対応するものではなく，時間経過に対応したり，空間のある場所から別の場所に移動する光子 — 光の粒子 — のような物理的粒子に対応することもある．回路に入力する状態は計算基底状態 — 通常はすべて $|0\rangle$ よりなる状態 — であると仮定するのが便利である．このルールは量子計算と

量子情報の文献でしばしば守られないことがあるが，そのときには読者に断るのが丁寧である．

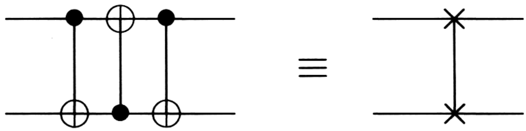


図 1.7: 2 つの q ビットを交換する回路と，それと等価なこの一般的で有用な回路に対する図式的記号．

図 1.7 の回路は簡単ではあるが有用なタスク — 2 つの q ビットの状態の入れ替え — を実行する．この回路が交換演算 (swap operation) を実行するのを見るために一連のゲートが計算基底状態 $|a,b\rangle$ に対して次のような一連の効果を与える．

$$\begin{aligned}|a,b\rangle &\to |a, a\oplus b\rangle \\ &\to |a\oplus(a\oplus b), a\oplus b\rangle = |b, a\oplus b\rangle \\ &\to |b, (a\oplus b)\oplus b\rangle = |b,a\rangle, \end{aligned} \tag{1.20}$$

ここですべての和は 2 を法とする和である．したがって，この回路の効果は 2 つの q ビット状態を交換することになる．

古典回路で許されるが量子回路には通常存在しないものが幾つかある．まず第 1 に「ループ」— つまり量子回路の一部から他の部分へのフィードバック — は許容されない．このとき回路は**非巡回的** (acyclic) であるという．第 2 に古典回路には配線が互いに「結合」して入力のビット毎の OR を含む 1 つの出力を与えるいわゆるファンイン (FANIN) と呼ぶ回路が存在する．明らかにこの演算は逆転可能ではなく，したがってユニタリーでないので，量子回路でファンインは許されない．第 3 にその逆演算 — ビットのコピーを幾つか作る — ファンアウト (FANOUT) も量子回路では許されない．実際量子力学では q ビットのコピーを作ることは禁止されており，ファンアウト演算を行うことは不可能である．次節で q ビットのコピー回路の作製を試みるときにこの例を調べる．

本書を読み進むに従い必要に応じて新しい量子ゲートを導入するが，この時点で量子回路に関するもう 1 つの約束事を紹介する．この約束を図 1.8 に示す．ここで U は n 個の q ビットに作用する**任意の**ユニタリー行列であり，したがって

U はこれら q ビットの量子ゲートと見なせるとする．このとき制御 NOT ゲートの自然な拡張として**制御 U** ゲート (controlled-U gate) を定義できる．このゲートは黒点を伴う線で表される単一の**制御 q ビット**と，箱に入った U で示される n 個の**標的 q ビット**より成っている．もしも制御 q ビットが 0 ならば標的 q ビットには何も起きない．もし制御 q ビットが 1 にセットされると標的 q ビットに対してゲート U が適用される．制御 U ゲートの原型が制御 NOT ゲートであり，図 1.9 に示すように $U = X$ とおいた制御 U ゲートに相当する．

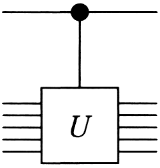


図 1.8: 制御 U ゲート．

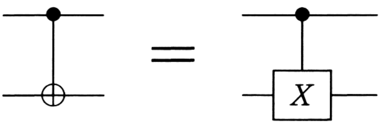


図 1.9: 制御 NOT に対する 2 つの異なる表現．

もう 1 つの重要な演算は測定であり，図 1.10 に示した「測定器」の記号で表示する．前に述べたようにこの演算は単一 q ビット状態 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ を確率的な古典ビット M — 2 重線で q ビットと区別する — に変換する．M は確率 $|\alpha|^2$ で 0，確率 $|\beta|^2$ で 1 である．

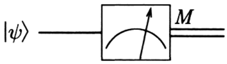


図 1.10: 測定の量子回路記号．

量子回路は計算や通信から量子雑音に至る量子プロセスのモデルとして有用であることがこれからわかるが，その用途はこれらに限られることはない．幾つかの簡単な例を次項以下に示す．

1.3.5 q ビットのコピー回路？

制御 NOT ゲートは特に量子情報の基本的性質を示すのに便利である．古典ビットをコピーするというタスクを考える．これを行うには図 1.11 に示すように古典的制御 NOT ゲートを使うことができて，コピーしたいビット（ある未知の状態 x）と 0 に初期化された「メモ用紙（一時記憶)」ビットを取り入れる．出力は 2 つのビットであり両方とも同じ状態 x になる．

同様に制御 NOT ゲートを用いて未知の状態 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ の q ビットのコピーを試みる．2 つの入力 q ビット状態は次のように書ける．

$$\left[a|0\rangle + b|1\rangle\right] |0\rangle = a|00\rangle + b|10\rangle, \tag{1.21}$$

制御 NOT 機能は最初の q ビットが 1 のとき第 2 の q ビットの符号を変えることであり，出力は $a|00\rangle + b|11\rangle$ となる．我々は首尾よくコピーできたであろうか？ つまり状態 $|\psi\rangle|\psi\rangle$ ができたであろうか？ $|\psi\rangle = |0\rangle$ または $|\psi\rangle = |1\rangle$ の場合にはこの回路が行っている通りであり，$|0\rangle$ または $|1\rangle$ と符号化された古典情報をコピーするのならば量子回路を使うことができる．しかし，一般の状態 $|\psi\rangle$ に対しては

$$|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ab|10\rangle + b^2|11\rangle. \tag{1.22}$$

$a|00\rangle + b|11\rangle$ と比べると，$ab = 0$ でなければ上の「コピー回路」は入力量子状態をコピーしたことにならない．実際に未知の量子状態のコピーを作るのは**不可能**であることがわかっている．q ビットはコピーできないというこの性質を**非クローン化定理** (複製不可能定理，no-cloning theorem) と呼び，これは量子情報と古典情報の主要な違いの 1 つである．非クローン化定理は 12 章（第 III 巻）のコラム 12.1 で詳しく議論する．証明は簡単なので今すぐにでも読んでみることを勧める．

図 1.11 の回路の失敗を調べるには，q ビットが測定にかからない何か「隠れた」情報をもっているという直観に基づく別の方法がある．状態 $a|00\rangle + b|11\rangle$ にある q ビットの 1 つを測定するとき何が起きるかを考える．前に述べたように確率 $|a|^2$ または $|b|^2$ で 0 または 1 が得られる．しかし，一度 1 つの q ビットが測定されると他の q ビットも完全に確定し，a と b に関するそれ以上の情報は得られない．この意味で元の q ビット $|\psi\rangle$ が持っていた付加的な隠れた情報は最初の測定

で失われて回復できない．しかし，もしqビットのコピーができたとすれば，他のqビットもその隠れた情報の一部を持っていなければならないことになる．したがってコピーをすることはできない．

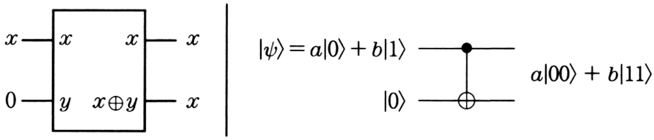


図 1.11: 未知のビットまたはqビットを「コピー」する古典回路と量子回路

1.3.6 例： Bell 状態

もう少し複雑な回路を考える．それは図1.12に示すようにHadamardゲートの後に制御NOTが続くもので，表に示すように4つの計算基底状態を変換する．実例をあげるとHadamardゲートは入力 $|00\rangle$ を $(|0\rangle+|1\rangle)|0\rangle/\sqrt{2}$ に変換し，制御NOTは出力状態 $(|00\rangle+|11\rangle)/\sqrt{2}$ を与える．この回路の働きを見てみよう．まずHadamard変換で最初のqビットの重ね合せが作られ，これが制御qビットとなって制御NOTに入力され，制御qビットが1のときにのみ標的qビットを反転する．出力状態は

$$|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}; \tag{1.23}$$

$$|\beta_{01}\rangle = \frac{|01\rangle+|10\rangle}{\sqrt{2}}; \tag{1.24}$$

$$|\beta_{10}\rangle = \frac{|00\rangle-|11\rangle}{\sqrt{2}}; \tag{1.25}$$

$$|\beta_{11}\rangle = \frac{|01\rangle-|10\rangle}{\sqrt{2}}; \tag{1.26}$$

で与えられる．このような状態の奇妙な性質を指摘したBellやEinstein, Podolsky, Rosenに因んで**Bell 状態** (Bell state)，あるいは時によって**EPR 状態** (EPR state)，**EPR 対** (EPR pair) とも呼ぶ．覚えやすいように $|\beta_{00}\rangle$，$|\beta_{01}\rangle$，$|\beta_{10}\rangle$，$|\beta_{11}\rangle$ は次式のようにまとめることができる．

$$|\beta_{xy}\rangle \equiv \frac{|0,y\rangle+(-1)^x|1,\bar{y}\rangle}{\sqrt{2}}, \tag{1.27}$$

ここで $\bar{y}$ は y の否定である．

入力	出力
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$

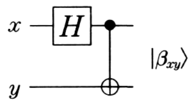


図 1.12: Bell 状態を作り出す量子回路と入出力状態を示す量子「真理値表」．

1.3.7 例： 量子テレポーテーション

これまで数頁にわたって学んだテクニックを使って，意義のある驚くべきかつ楽しみの多い話題 — 量子テレポーテーション— を調べてみよう！ 量子テレポーテーションは量子状態の発信者と受信者の間を結ぶ量子通信チャンネルがなくても量子状態を移動させるテクニックである．

量子テレポーテーションはこのような働きをする： Alice と Bob は昔出会ったことがあるが今は遙か離れて住んでいる．一緒にいるときに彼らは EPR 対を生成し，それぞれが EPR 対のうちの 1 個の q ビットを持って別れた経緯がある．何年か経って隠れた場所にいる Bob に，$|\psi\rangle$ なる q ビットを届ける役目が Alice に任された．彼女は q ビットの状態が何であるか知らないうえに，Bob に**古典的情**報しか送ることができない．Alice はその役目を引き受けるべきか？

直観的にいって事情は Alice にとってかなり良くない．彼女は Bob に送るべき q ビットの状態 $|\psi\rangle$ を知らないし，彼女だけが $|\psi\rangle$ のコピーを持っているときに，量子力学の法則によってその状態を決めることはできない．さらに悪いことにもし彼女が $|\psi\rangle$ の状態を知ったとしても，$|\psi\rangle$ が連続空間の値をとるのでそれを正確に記述するには無限に多くの古典情報を必要とする．したがって，彼女が $|\psi\rangle$ を知ってもそれを Bob に伝えるには無限の時間がかかる．Alice にとって事態は悪そうである．しかし，Alice にとって幸運なことに量子テレポーテーションはわずかな古典通信の負担だけで，もつれ合った EPR 対を使って $|\psi\rangle$ を Bob に送る方法なのである．この解に至るステップの概要は次の通りである．Alice は q ビット $|\psi\rangle$ と彼女が持っている EPR 対の半分とを相互作用させ，手許にある 2 つの q ビットを測定して 4 つの可能な古典的結果 00，01，10，11 のうちの 1 つを得る．

彼女はその情報を Bob に送る．Alice からの古典的メッセージに応じて，Bob は 4 つの演算の 1 つを彼が持っている EPR 対の半分に施す．驚くべきことにこれを行うと元の状態 $|\psi\rangle$ が再生できるのである！

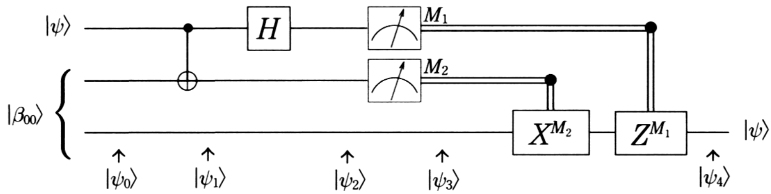


図 1.13: q ビットをテレポートする量子回路．上の 2 つの線は Alice のシステム，下の線は Bob のシステムを表す．測定器は測定を表しそこから出てくる 2 重線は古典ビット，その他の単線は q ビットを表す．

図 1.13 に示す量子回路は量子テレポーテーションを正確に記述している．テレポーテーションで送るべき状態は $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$，$\alpha$ と β は未知の振幅である．回路への入力状態 $|\psi_0\rangle$ は．

$$|\psi_0\rangle = |\psi\rangle\ |\beta_{00}\rangle \tag{1.28}$$

$$= \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|00\rangle + |11\rangle)\Big], \tag{1.29}$$

ここで最初の（左の）2 つの q ビットは Alice のもの，3 番目の q ビットは Bob のものという慣用に従う．前に説明したように Alice の 2 番目の q ビットと Bob の q ビットは EPR 状態から出発したものである．Alice が彼女の q ビットを制御 NOT ゲートに通すと，

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle + |11\rangle) + \beta|1\rangle(|10\rangle + |01\rangle)\Big]. \tag{1.30}$$

次に最初の q ビットを Hadamard ゲートに通すと，

$$|\psi_2\rangle = \frac{1}{2}\Big[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)\Big]. \tag{1.31}$$

この状態の項をグループ分けし直すと，次のように書き直せる．

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)$$
$$+ |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big]. \tag{1.32}$$

この式は 4 つの項より成る．第 1 項は Alice の q ビットが状態 $|00\rangle$，Bob の q ビットが状態 $\alpha|0\rangle+\beta|1\rangle$ — これは元の状態 $|\psi\rangle$ — である．もし Alice が測定で結果 00 を得れば Bob のシステムは状態 $|\psi\rangle$ にある．同様に上の式から Bob の測定後の状態を読み取ることができる．Alice の測定結果が与えられると

$$00 \longmapsto |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle], \tag{1.33}$$

$$01 \longmapsto |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle], \tag{1.34}$$

$$10 \longmapsto |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle], \tag{1.35}$$

$$11 \longmapsto |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle]. \tag{1.36}$$

Alice の測定出力に依存して Bob の q ビットは最後にこれら 4 つの可能な状態となっている．もちろんどの状態にあるべきかを知るために Bob は Alice の測定結果を知らねばならない — この事実があるためにテレポーテーションで情報を光速より速く送れないことを後で示す．ひとたび Bob が測定結果を教わると Bob は適当な量子ゲートを作用させて彼の状態を決定して $|\psi\rangle$ を再現することができる．例えば，測定結果が 00 ならば Bob は何もしなくてよい．測定結果が 01 ならば Bob は X ゲートを適用して彼の状態を決定する．測定結果が 10 ならば Bob は Z ゲートを適用して彼の状態を決定する．測定結果が 11 ならば Bob は最初に X ゲート，次に Z ゲートを適用する．まとめると，Bob が彼の q ビットに変換 $Z^{M_1}X^{M_2}$ を適用（回路図では時間は左から右に経過するが，行列積では右の因子が先に生じることに注意）すると $|\psi\rangle$ が回復できる．

量子テレポーテーションには多くの興味ある性質があるが，それらについては後の部分にゆずることにする．ここでは 2 つの側面についてコメントするにとどめる．第 1 にテレポーテーションは量子状態を光速より速く伝送するのではないか？ 相対論によれば光より速い情報伝達をするには，情報を時間に逆らって送らねばならないのでこの疑問は少し異常である．幸運なことにテレポーテーションを完成させるために，Alice は古典通信で Bob に測定結果を伝送しなければならないから，量子テレポーテーションは光より速い通信を可能にするものではない．2.4.3 項において古典通信なしには，テレポーテーションで**如何なる**情報も伝えることができないことを示す．古典チャンネルは光速で制限されているので，量子テレポーテーションも光速より速く行うことができず，見かけ上のパラドックス

は解決される．

テレポーテーションに関する第2のパズルは，テレポートされる状態のコピーを作っているように見えることであり，明らかに1.3.4項で議論した非クローン化定理を破っている．この違反は錯覚に基づくものであって，テレポーテーション過程の後では標的qビットだけが $|\psi\rangle$ 状態に残り，最初のqビットの測定結果に依存して元のデータqビットは計算基底状態 $|0\rangle$ か $|1\rangle$ のいずれか一方になっている．

量子テレポーテーションから学ぶべきものは何か？ 極めて多い！ それは量子状態を使った巧妙なトリック以上のものである．量子テレポーテーションは量子力学の**異なる**リソースが交換可能であることを強調しており，1つの共有されたEPR対と2ビットの古典通信が少なくとも1個のqビット通信と等価なリソースであることを示している．量子計算と量子情報ではリソースを交換する多くの方法が示されており，その多くが量子テレポーテーションに基づいている．具体的に10章（第III巻）でテレポーテーションを用いた雑音効果に耐性を持つ量子ゲートの作り方を説明し，12章（第III巻）でテレポーテーションが量子誤り訂正符号の性質に密接に関係していることを示す．他の問題とこのように関係が深いにもかかわらず，正直のところ量子力学において量子テレポーテーションが可能なのがなぜなのか我々は理解し始めたばかりである．後の章でそのような理解を可能にする幾つかの洞察について説明する．

1.4　量子アルゴリズム

量子回路を用いてどのようなクラスの計算ができるか？ その計算は古典論理回路を使ってできる計算に比べてどうか？ 古典コンピュータよりも量子コンピュータがうまくできる計算タスクは見つかるか？ この節ではこれらの疑問について調べて，量子コンピュータ上で古典計算を行う方法を説明する．量子コンピュータが古典コンピュータに比べて有利になる問題を幾つか例示し，最後に既知の量子アルゴリズムをまとめる．

1.4.1 量子コンピュータ上での古典計算

量子回路を用いて古典論理回路をシミュレートできるか？ 驚くには当たらないがこの疑問に対する答えは yes である．物理学者は古典論理回路も含めて我々の回りのあらゆるものが最終的に量子力学で説明できると信じているので，もしそうでなければむしろ非常に驚くべきことである．前に指摘したように量子回路を使って古典回路を直接シミュレートできない理由は，ユニタリーな量子論理ゲートが本質的に**可逆**であるのに対して，NAND ゲートのような多くの古典論理回路が本来非可逆であるからである．

Toffoli ゲート(Toffoli gate) と呼ぶ可逆ゲートを用いれば，如何なる古典回路も**可逆**要素のみを用いた等価回路に置き換えられる．図 1.14 に示すように Toffoli ゲートは 3 つの入力ビットと 3 つの出力ビットを持っている．このうちの 2 つは**制御ビット**であり Toffoli ゲートの作用によって影響を受けない．第 3 ビットは**標的ビット**であって，2 つの制御ビットが共に 1 ならば反転し，そうでなければ変化しない．Toffoli ゲートを 2 回作用させると $(a,b,c) \to (a,b,c\oplus ab) \to (a,b,c)$ となり，したがって Toffoli ゲートは逆のゲート — つまりそれ自身 — を持つので可逆である．

入力			出力		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

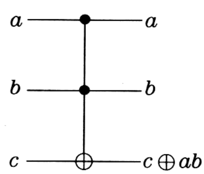


図 1.14: Toffoli ゲートの真理値表と回路表示．

Toffoli ゲートを用いると図 1.15 に示す NAND ゲートと図 1.16 に示すファンアウトのシミュレーションができる．他の古典回路の全要素がこれら 2 つの演算によってシミュレーションできるので，任意の古典回路が等価な可逆回路によりシミュレートできることになる．

Toffoli ゲートを古典ゲートとして述べてきたが，これは量子論理ゲートとして

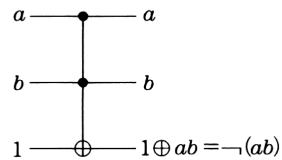


図 1.15: Toffoli ゲートを用いて作った古典回路の NAND ゲート．上の 2 つのビットが NAND への入力を表し，第 3 のビットに標準状態 1 — **補助状態**(ancilla state) と呼ばれる — を入力する．NAND 出力は第 3 ビットに現れる．

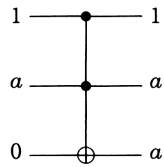


図 1.16: Toffoli ゲートによるファンアウト．第 2 ビットがファンアウト入力（他の 2 つは標準補助状態），ファンアウト出力は第 2 と第 3 ビットに出る．

も実行できる．Toffoli ゲートを量子論理として実行すると，古典的 Toffoli ゲートと同様に，定義により計算基底状態が単純に置換される．例えば，状態 $|110\rangle$ に Toffoli ゲートが作用すると，最初の 2 つが 1 だから第 3 の q ビットが反転して状態 $|111\rangle$ となる．この変換を 8×8 の行列 U で表し，U がユニタリー行列であることを明示的に証明し，したがって Toffoli ゲートが合理的量子ゲートであることを示すのは退屈であるが困難ではない．古典的 Toffoli ゲートと同様に量子 Toffoli ゲートを使って非可逆な古典論理ゲートをシミュレートできて，（決定性の）古典コンピュータにできるどんな計算も量子コンピュータで実行できることが保証される．

もし古典コンピュータが非決定性ならば — つまり計算に使用する乱数ビットを発生する能力を持っていたら — どうなるか？ 驚くまでもなく量子コンピュータはこれもシミュレートできる．このシミュレーションを実行するにはランダムにコイン投げを行えばよく，それを実行するには状態 $|0\rangle$ の q ビットを用意して Hadamard ゲートを通して状態 $(|0\rangle + |1\rangle)/\sqrt{2}$ を作り，次にその状態を測定すればよい．結果は 50%/50% で $|0\rangle$ か $|1\rangle$ となる．これにより量子コンピュータは非決定性古典コンピュータを効率良くシミュレートできる能力を持つ．

もちろん，もし古典コンピュータをシミュレートする能力が量子コンピュータ

の唯一の特徴ならば，量子効果の活用という面倒なことを行うご利益はあまりない！ 量子コンピュータの利点は q ビットと量子ゲートを用いることによって，はるかに強力な関数が計算できることにある．次の数項では如何にこれを行うかを説明し，古典コンピュータより速く問題を解くことができる量子アルゴリズムの最初の例として，Deutsch-Jozsa のアルゴリズムを説明する．

1.4.2 量子並列性

量子並列性 (quantum parallelism) とは多くの量子アルゴリズムの基本的性質である．経験的にかつ過度に単純化するリスクを恐れずに言えば，量子コンピュータは量子並列性によって多くの**異なる** x に対して，同時に関数 $f(x)$ を評価することができる．本項では量子並列性の働きと，幾つかの制約について説明する．

$f(x) : \{0,1\} \to \{0,1\}$ は 1 ビットの定義域と値域を持つ関数であると想定する．この関数を量子コンピュータで計算する便利な方法として，状態 $|x, y\rangle$ から出発する 2 つの q ビットの量子コンピュータを考える．適切な一連の論理ゲートを用いるとこの状態は $|x, y \oplus f(x)\rangle$ に変換できる．ここで $\oplus$ は 2 を法とする和を表す．最初のレジスタを「データ」レジスタ，2 番目のレジスタを「標的」レジスタと呼ぶ． 写像：$|x, y\rangle \to |x, y \oplus f(x)\rangle$ で定義する変換を U_f と名付ける．U_f がユニタリーであることは容易に証明できる．もし $y = 0$ ならば第 2 の q ビットの最終状態の値は $f(x)$ である．（3.2.5 項で f を計算する古典回路が与えられれば量子コンピュータ上で変換 U_f を同程度の効率で計算する量子回路が存在することを示す．我々の目的には U_f はブラックボックスと考えてよい．）

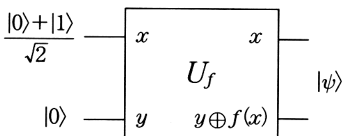


図 1.17: $f(0)$ と $f(1)$ を同時に評価する量子回路．U_f は $|x, y\rangle$ のような入力を $|x, y \oplus f(x)\rangle$ に変換する量子回路．

図 1.17 に示すように計算基底でない重ね合せ状態入力に対して，U_f を適用する回路を考える．あるいは $|0\rangle$ に Hadamard ゲートを作用させると重ね合せ

$(|0\rangle+|1\rangle)/\sqrt{2}$ が得られるので，これをデータレジスタに入れてもよい．U_f を適用すると次の結果を得る．

$$\frac{|0, f(0)\rangle+|1, f(1)\rangle}{\sqrt{2}} \tag{1.37}$$

これは注目すべき状態である！ 異なる項が $f(0)$ と $f(1)$ の両方に関する情報を含み，あたかも2つの x の値に対する $f(x)$ を計算したかのようなので，この特徴を「量子並列性」と呼ぶ．$f(x)$ を計算する回路を複数個持つ古典的並列性とは異なり，ここでは異なる状態の重ね合せを表現できる量子コンピュータの能力を活用して，単一の回路で複数値の x に対して関数を計算できる．

この手続きは **Hadamard 変換** (Hadamard transform) または **Walsh-Hadamard 変換** (Walsh-Hadamard transform) と呼ぶ一般的演算を使えば任意ビット数の関数に容易に拡張できる．この演算は n 個のqビットに並列に作用する n 個の Hadamard ゲートにほかならない．例えば，図1.18は $|0\rangle$ に初期化された $n=2$ のqビットに対するものであり，その出力は

$$\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)=\frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2} \tag{1.38}$$

で与えられる．Hadamard ゲートの並列作用を $H^{\otimes 2}$ と表し，「$\otimes$」は「テンソル」と読む．一般化するとすべて $|0\rangle$ 状態に初期化された n 個のqビットに Hadamard 変換を施すと，その結果は：

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle, \tag{1.39}$$

ここで総和は x がとり得るすべての（n ビットの）値 x に対して行い，この演算を $H^{\otimes n}$ と表す．すなわち，Hadamard 変換によりすべての計算基底状態の対等な重ね合せを作り出すことができ，しかも 2^n 個の状態の重ね合せをわずか n 個のゲートで実現できるので極めて効率が良い．

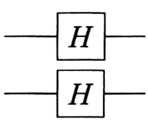


図 1.18: 2つのqビットに作用する Hadamard 変換 $H^{\otimes 2}$.

n ビットの入力 x と 1 ビットの出力を有する関数 $f(x)$ の量子並列計算は次のように行う．$n+1$ 個の q ビット状態 $|0\rangle^{\otimes n}|0\rangle$ を準備して，最初の n 個の q ビットに Hadamard 変換を適用し，次に U_f の機能を持つ量子回路を通す．これにより次の状態が作り出される．

$$\frac{1}{\sqrt{2^n}}\sum_x |x\rangle|f(x)\rangle. \tag{1.40}$$

ある意味で一見関数 f を 1 回しか計算していないにもかかわらず，量子並列性により f のすべての可能な値を同時に計算することができる．しかし，この並列性が直ちに有用というわけではない．つまり単一 q ビットの例でいえは状態測定により単に $|0,f(0)\rangle$ か $|1,f(1)\rangle$ の**いずれか**が得られるにすぎない！ 同様に一般の場合でも状態 $\sum_x |x,f(x)\rangle$ の測定で x の 1 つの値に対する $f(x)$ が得られるにすぎない．もちろん，これなら古典コンピュータで容易にできる！ 量子計算には単なる量子並列性以上の何か有用なもの，つまり $\sum_x |x,f(x)\rangle$ のような重ね合せ状態から 2 つ以上の $f(x)$ の値に関する情報を抽出する能力が望まれる．これができる方法の例を次の 2 項で調べる．

1.4.3 Deutsch のアルゴリズム

図 1.17 の回路を少し変更すると **Deutsch のアルゴリズム** (Deutsch algorithm) を使って，古典回路を凌ぐ働きを量子回路にさせることができる（実際に示すのは元のアルゴリズムを単純化した改良版である．章末の「歴史と参考資料」参照）．Deutsch のアルゴリズムは量子並列性と，量子力学の性質である**干渉** (interference) を組み合わせたものである．前と同様に Hadamard ゲートを用いて重ね合せて初期 q ビット $(|0\rangle+|1\rangle)/\sqrt{2}$ を作るが，今回はさらに Hadamard ゲートを $|1\rangle$ にも適用して第 2 の q ビット y を重ね合せ状態 $(|0\rangle-|1\rangle)/\sqrt{2}$ とする．図 1.19 に示すこの回路で何が起きるか状態の変化をたどってみる．

入力状態：

$$|\psi_0\rangle = |01\rangle \tag{1.41}$$

は 2 つの Hadamard ゲートによって次のように変換される：

$$|\psi_1\rangle = \left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right] \tag{1.42}$$

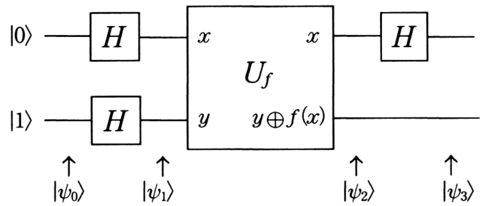


図 1.19: Deutsch のアルゴリズムを実行する量子回路.

少し考えると状態 $|x\rangle(|0\rangle - |1\rangle)/\sqrt{2}$ に対して U_f を作用させると，状態 $(-1)^{f(x)}|x\rangle\ (|0\rangle - |1\rangle)/\sqrt{2}$ が得られることがわかる．U_f を $|\psi_1\rangle$ に作用させると 2 つの可能性のうちの一方が得られる．

$$|\psi_2\rangle = \begin{cases} \pm\left[\dfrac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)=f(1)\ \text{のとき}, \\ \pm\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right]\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)\neq f(1)\ \text{のとき}. \end{cases} \tag{1.43}$$

第 1 - q ビットに対する Hadamard ゲートの出力は

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)=f(1)\ \text{のとき}, \\ \pm|1\rangle\left[\dfrac{|0\rangle-|1\rangle}{\sqrt{2}}\right], & f(0)\neq f(1)\ \text{のとき}. \end{cases} \tag{1.44}$$

$f(0)=f(1)$ ならば $f(0)\oplus f(1)=0$，そうでなければ 1 なので，この結果を簡潔にまとめると

$$|\psi_3\rangle = \pm|f(0)\oplus f(1)\rangle\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right], \tag{1.45}$$

したがって，第 1 - q ビットを測定すると $f(0)\oplus f(1)$ を決めることができる．これは実は非常に興味深いことであり，量子回路は $f(x)$ をたった **1 回**測定するだけで $f(x)$ の**全体の性質**，つまり $f(0)\oplus f(1)$ を決める能力を我々に与える！ これは少なくとも 2 回の測定が必要な古典的装置よりも速い．

この例は量子並列性と古典的な確率的アルゴリズムの違いを際立たせている．単純にみれば状態 $|0\rangle|f(0)\rangle+|1\rangle|f(1)\rangle$ は 1/2 の確率で $f(0)$，1/2 の確率で $f(1)$

を計算する確率的古典コンピュータとむしろ密接に対応している．違いは古典コンピュータではこの2つの選択肢が互いに排他的であるのに対して，量子コンピュータでは Hadamard ゲート等により異なる選択肢が結合され，2つの選択肢が互いに**干渉** (interfere) して関数 f の全体の様相を生み出している．これが Deutsch のアルゴリズムで行われている．多くの量子アルゴリズム設計の本質は関数と最終的な変換をうまく選ぶことにより，— 古典コンピュータでは素早く得ることができない — その関数全体の有用な情報を効率良く決定できることにある．

1.4.4　Deutsch-Jozsa のアルゴリズム

Deutsch のアルゴリズムは Deutsch-Jozsa のアルゴリズムと呼ぶ一般的量子アルゴリズムの最も簡単な場合に相当する．**Deutsch の問題** (Deutsch's problem) として知られている応用は次のようなゲームの形で述べることができる．アムステルダムにいる Alice が数 x を 0 から 2^n-1 の中から選び，ボストンにいる Bob に手紙で知らせる．Bob はある関数 $f(x)$ を計算しその結果 — 0 または 1 — を返事する．さて Bob はあらかじめ2種類の関数のうちのいずれか一方を使うと約束していたとする．その関数の1つは x の如何にかかわらず常に**一定値**であり，もう1つは**バランス** した関数，つまりすべての可能な x の丁度半分の x に対して1その他の x に対して0となる関数である．Alice の目的は互いの通信を最小限に保ったうえで Bob が一定値型を選んだか，バランス型を選んだかを確実に決定することである．彼女は如何に速く決められるか？

古典的場合には Alice は Bob に一通の手紙当たり x の値を1つだけ送ることができる．Bob の関数がバランス型であることが最終的にわかるには $2^n/2$ 回だけ0の返事が必要なので，Alice は少なくとも $2^n/2+1$ 回質問しなければならない．つまり，彼女が使える最良の古典的な決定性アルゴリズムでは，$2^n/2+1$ 回の質問が必要である．Alice は Bob に一通の手紙当たり n ビットの情報を送らねばならないことに注意する．そのうえ，この例では物理的な距離をわざと長くして $f(x)$ の計算コストが高くつくようにしたが，$f(x)$ の計算が本来困難な一般の問題ではこのようなことは必要でない．

もし Bob と Alice が古典ビットの代わりに q ビットを交換することができて，Bob が $f(x)$ の計算にユニタリー変換 U_f を用いることに同意するならば，Alice

は次のアルゴリズムを用いて**1回**の通信だけで目的を達成できる．

Deutsch のアルゴリズムと同様に，Alice は質問を蓄える n 個の q ビットレジスタを持っており，回答を蓄える 1 個の q ビットレジスタを Bob に与える．最初に彼女は質問と回答のレジスタを重ね合せ状態にする．Bob は量子並列性を用いて $f(x)$ を計算し，その結果を回答レジスタに入れる．次に Alice は Hadamard 変換を使って重ね合せ状態を質問レジスタ状態と干渉させ，適切な測定を使って f が一定値型かバランス型かを決定する．

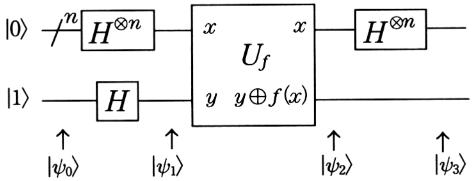


図 1.20: 一般的 Deutsch-Jozsa のアルゴリズムを実行する量子回路．記号「/」のある配線は技術の記号と同様に n 個の q ビットの集合を表す．

アルゴリズムの具体的ステップを図 1.20 に示す．この回路に沿って状態の推移を追ってみよう．入力状態：

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle \tag{1.46}$$

は式 (1.41) と似ているが，ここでは質問レジスタの n 個の q ビットはすべて $|0\rangle$ 状態に準備されている．質問レジスタに Hadamard 変換を施し，回答レジスタの内容を Hadamard ゲートを通すと，

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{1.47}$$

この結果質問レジスタはすべての値の重ね合せとなり，回答レジスタは 0 と 1 の等加重の重ね合せとなる．次に Bob が $U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$ を用いて関数 f を計算する：

$$|\psi_2\rangle = \sum_{x} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]. \tag{1.48}$$

Alice は Bob の関数評価の結果が q ビットの重ね合せ状態の振幅として蓄積されている q ビットを 1 セット手に入れたことになる．次に彼女は質問レジスタに

Hadamard 変換を施し，重ね合せ項を干渉させる．Hadamard 変換の結果を求めるには，まず状態 $|x\rangle$ を Hadamard 変換する効果を計算する．$x=0$ と $x=1$ の場合を別々にチェックすると，単一 q ビットに対して $H|x\rangle = \sum_z (-1)^{x\cdot z}|z\rangle/\sqrt{2}$ である．したがって

$$H^{\otimes n}|x_1,\ldots,x_n\rangle = \frac{\sum_{z_1,\ldots,z_n}(-1)^{x_1z_1+\ldots+x_nz_n}|z_1,\ldots,z_n\rangle}{\sqrt{2^n}}. \tag{1.49}$$

これを簡潔にまとめると有用な式が得られる．

$$H^{\otimes n}|x\rangle = \frac{\sum_z(-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}, \tag{1.50}$$

ここで $x\cdot z$ は 2 を法とする x と z のビット毎の内積である．この式と式 (1.48) を用いると $|\psi_3\rangle$ が求まる．

$$|\psi_3\rangle = \sum_z\sum_x \frac{(-1)^{x\cdot z+f(x)}|z\rangle}{2^n}\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]. \tag{1.51}$$

Alice は次に質問レジスタを見る．状態 $|0\rangle^{\otimes n}$ の振幅は $\sum_x(-1)^{f(x)}/2^n$ である．何が起きるか — 一定値形 f とバランス形 f の — 2 つの可能な状態を見てみよう．f が一定値形の場合 $|0\rangle^{\otimes n}$ の振幅は，$f(x)$ がとる一定値に応じて $+1$ または -1 である．$|\psi_3\rangle$ の長さは 1 なので他の全振幅は 0 でなければならず，質問レジスタの全 q ビットに対して観測値 0 を与える．もしも f がバランス形ならば $|0\rangle^{\otimes n}$ の振幅に対する正と負の寄与が相殺して振幅が 0 になり，測定すると質問レジスタ中の少なくとも 1 つの q ビットが 0 以外の結果を与えなければならない．以上をまとめると Alice の測定結果がすべて 0 ならば関数は一定値形，そうでなければバランス形である．Deutsch-Jozsa のアルゴリズムを以下にまとめておく．

Deutsch-Jozsa のアルゴリズム：

入力： $x\in\{0,\ldots,2^n-1\}$ と $f(x)\in\{0,1\}$ に対して変換 $|x\rangle\,|y\rangle\to|x\rangle|y\oplus f(x)\rangle$ を行うブラックボックス U_f が与えられる．前提として $f(x)$ はすべての x に対して**一定値形**であるか，さもなければ $f(x)$ は **バランス形**である — つまり x のすべてのとり得る値の丁度半分に対して 1 に等しく，他のすべての半分に対して 0 に等しい — ことが約束されている．

出力：　f が一定形であるときにのみ 0.

演算回数：　U_f を一回測定．常に成功.

手続き：

1.	$\|0\rangle^{\otimes n}\|1\rangle$	状態を初期化
2.	$\rightarrow \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \|x\rangle \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	Hadamrad ゲートで重ね合せを作成
3.	$\rightarrow \frac{1}{\sqrt{2^n}} \sum_x (-1)^{f(x)} \|x\rangle \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	U_f を用い関数 f を計算
4.	$\rightarrow \sum_z \sum_x \frac{(-1)^{x\cdot z+f(x)}\|z\rangle}{2^n} \left[\frac{\|0\rangle - \|1\rangle}{\sqrt{2}}\right]$	Hadamard 変換を実行
5.	$\rightarrow z$	測定で出力 z を得る

古典コンピュータで $2^n/2+1$ 回の計算が必要であるのに対して，量子コンピュータでは関数 f を 1 回計算することによって，Deutsch の問題が解けることを示した．これは一見感銘を与えるものであるが，注意すべき重要な点が幾つかある．1 つには Deutsch の問題が特に重要な問題というわけではなく，その応用は見つかっていない．2 番目には古典アルゴリズムと量子アルゴリズムの比較は，ある意味でリンゴとオレンジの比較のようなもので，両方の場合の関数の計算法がまるで異なる．3 番目にもし Alice に確率的な古典コンピュータを使うことが許されれば，ランダムに選んだ二三の x の値に対して $f(x)$ を計算するよう Bob に依頼すれば彼女は高い確率で f が一定値型かバランス型かを速やかに決定できる．この確率論的シナリオは我々が考えてきた決定性シナリオにより現実的である．これら注意点があるにもかかわらず，Deutsch-Jozsa のアルゴリズムはもっと感銘深い量子アルゴリズムの種を宿しており，この演算の裏にある原理を理解することは有用である．

演習 1.1:（確率論的な古典アルゴリズム） 一定値形関数とバランス形関数の区別を**確定的**に区別するのではなく，ある誤り確率 $\epsilon < 1/2$ で区別する問題があるとする．この問題に対する最良の古典アルゴリズムの性能はどうなるか？

1.4.5 量子アルゴリズムのまとめ

Deutsch-Jozsa のアルゴリズムは，古典コンピュータに比べて量子コンピュータが，幾つかの計算問題を効率的に解けることを示唆している．残念ながら解ける問題に応用上の興味はあまりない．量子アルゴリズムを用いてより効率的に解けて，しかも興味深い問題はないか？ このようなアルゴリズムに潜む原理は何か？ 量子コンピュータの計算能力の究極的限界は何か？

大雑把に言えば，既知の古典アルゴリズムに比べて有利な量子アルゴリズムには三つのクラスがある．1 つは古典アルゴリズムでも広く用いられるツールである，Fourier 変換の量子版をベースにしたアルゴリズムのクラスである．Deutsch-Jozsa のアルゴリズムはこのクラスの例であり，Shor の素因数分解や離散対数アルゴリズムもこれに属する．第 2 のクラスは量子探索アルゴリズムである．第 3 のクラスは量子シミュレーションであり，量子コンピュータを用いて量子システムのシミュレーションを行う．これらのクラスのアルゴリズムについて簡単に述べて，量子コンピュータの計算能力について何がわかっており，何が問題なのかをまとめる．

Fourier 変換をベースとするアルゴリズム

離散的 Fourier 変換は N 個の複素数集合 $x_0, \ldots, x_{N-1}$ を別の複素数集合 $y_0, \ldots, y_{N-1}$ に変換するもので

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{2\pi ijk/N} x_j \tag{1.52}$$

で定義する．もちろんこの変換は科学の多くの分野で広く応用されている．元の問題を直接解くより，Fourier 変換をしてから解くほうが解が得やすいことが多い．

Fourier 変換は非常に有用なので，式 (1.52) の定義式を越えて Fourier 変換の美しい一般理論が作られている．この一般論には有限群の指標理論 (character theory) に基づく，テクニカルな概念が含まれているがここではあえて述べない．重要なことは Deutsch-Jozsa のアルゴリズムに用いられた Hadamard 変換がこの一般化された Fourier 変換の一例であることである．さらに付け加えれば，他の多くの重要な量子アルゴリズムも何らかの形の Fourier 変換を含んでいる．

今知られている最も重要な量子アルゴリズムである，Shor の素因数分解と離散対数の高速アルゴリズムは，式 (1.52) で定義される Fourier 変換を基にしているものの例である．式 (1.52) はこれまで書いてきたようないかにも量子力学的な式の格好をしていない．しかし n 個の q ビットに作用する線形変換 U を計算基底状態 $|j\rangle$ に対する次の操作で定義することを考える．

$$|j\rangle \to \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle. \tag{1.53}$$

ここで $0 \le j \le 2^n - 1$ である．この変換はユニタリーであり，実際に量子回路で実現できることが確認できる．さらにこの操作を重ね合せで書き下せば，

$$\sum_{j=0}^{2^n-1} x_j |j\rangle \to \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left[\sum_{j=0}^{2^n-1} e^{2\pi ijk/2^n} x_j \right] |k\rangle = \sum_{k=0}^{2^n-1} y_k |k\rangle, \tag{1.54}$$

これは $N = 2^n$ の場合に対する Fourier 変換 (1.52) のベクトル表記に相当することがわかる．

Fourier 変換をどれくらい速く実行できるであろうか？ 古典的には $N = 2^n$ 個の数を高速 Fourier 変換するのにざっと $N \log N = n2^n$ ステップを要する．量子コンピュータでは $\log^2(N) = n^2$ ステップで Fourier 変換をすることができて，指数関数的な節約になる！ これを行う量子回路を 5 章で説明する．

この結果によれば，2^n 個の複素数ベクトルを高速 Fourier 変換するのに量子コンピュータを用いることができて，広範囲の用途に途方もなく有用であるように見える．しかし Fourier 変換は量子状態の振幅に「隠れた」情報に対して行われるので，実際にこうは行かない．つまりこの情報を直接測定することができない．もちろん落とし穴は出力を測定すると，各 q ビットの状態が収縮して $|0\rangle$ または $|1\rangle$ になることにあり，変換の結果 y_k を直接知ることができない．この例は量子アルゴリズムを考案する難問の核心に迫るものである．一方では n 個の q ビットに関する 2^n 個の振幅について，ある種の計算を古典コンピュータよりもはるかに効率良く行うことができる．しかし他方では，我々が直接的方法で行ってもその計算結果を手に入れることはできず，量子計算を利用するには手際良さが要求される．

幸いなことに古典コンピュータで解を求める効率的方法がないと信じられている幾つかの問題を，量子 Fourier 変換を用いて効率良く解くことができることがわかっている．このような問題には Deutsch の問題や，離散対数と素因数分解に関する Shor のアルゴリズムが含まれる．この一連の考えの行き着くところが **Abel の固定部分群問題** (Abelian stabilizer problem) を解く Kitaev の方法の発見と，それを一般化した次に示す**隠れ部分群問題** (hidden subgroup problem) である．

> f は有限生成群 G から有限集合 X へ写像する関数であり，部分群 K の剰余類 (coset) 上で一定，各剰余類で互いに異なるとする．ユニタリー変換 $U|g\rangle|h\rangle = |g\rangle|h \oplus f(g)\rangle$ を実行する量子ブラックボックスが与えられたとき， K に対する生成集合を求めよ．ここで $g \in G$, $h \in X$, $\oplus$ は X に作用する適切に選ばれた 2 進オペレータとする．

Deutsch-Jozsa のアルゴリズム，Shor のアルゴリズム，およびこれに関連する「指数関数的に高速な」アルゴリズムはすべてこのアルゴリズムの特殊例と見なせる．量子 Fourier 変換とその応用は 5 章（第 II 巻）で述べる．

量子探索アルゴリズム

全く異なるクラスのアルゴリズムの代表格が量子探索アルゴリズムであり，その基本原理は Grover により見出された．量子探索アルゴリズムが解けるのは次のような問題である：サイズ N の探索空間が与えられ，その中の情報の構造に関してあらかじめ与えられた知識はないとする．その空間から既知の性質を持つ要素を探索したい．その性質を満たす要素を見出すにはどれくらい長くかかるか？古典的にはこの問題を解くにはほぼ N 回の演算を必要とするが，量子探索アルゴリズムではおよそ $\sqrt{N}$ 回の演算でよい．

量子 Fourier 変換に基づくアルゴリズムにおける感銘的な指数関数的高速化と異なり，量子探索アルゴリズムの高速化は 2 乗程度にすぎない．しかしそれでも量子 Fourier 変換で解ける問題に比べて，この発見的探索法は幅広い応用範囲を持っている．量子探索アルゴリズムを採用すると非常に広範囲の問題に実益がありそうなので，これは十分に興味をそそるものである．量子探索アルゴリズムとその応用については 6 章（第 II 巻）で述べる．

量子シミュレーション

自然界に生起する量子力学システムのシミュレーションは未だに古典コンピュータで困難と考えられており，明らかに量子コンピュータが勝る可能性がある．古典コンピュータが量子コンピュータをシミュレートするのが難しいのと全く同じ理由で，— システムサイズが大きくなるに従って古典的システムが線形的に増加するのと異なり，量子システムを記述する複素数の数が**指数関数的**に増加するので — 一般的量子システムをシミュレートするのが困難である．一般に n 個の異なる要素を持つシステムの量子状態を記憶するには，古典コンピュータ上で c^n ビット程度のメモリを必要とする．ここで c はシミュレーションの対象システムの詳細と，シミュレーション精度で決まる定数である．

これと対照的に，量子コンピュータでは kn 個の q ビットを用いてシミュレーションできる．ここでも k はシミュレーションするシステムの詳細に依存する定数である．これにより古典コンピュータでは効率が悪い量子力学的システムのシミュレーションを，量子コンピュータで効率良く実行できる．重要なことを1つ注意しておくと，古典コンピュータに比べて量子コンピュータが遙かに効率良く多くの量子システムをシミュレートできるとはいえ，量子システムの希望する情報が高速シミュレーションにより得られることは意味しない．測定が済むと kn 個の q ビットのシミュレーションは収縮して確定状態となり，kn ビットの情報しか与えない．つまり，波動関数に含まれる c^n ビットの「隠れた情報」には全くアクセスできないのである．このようなわけで量子シミュレーションを有益なものにするための重要なステップは，希望する答えを効率良く引き出せる系統的な手法を開発することである．どうすればよいかはほんの一部しかわかっていない．

このような注意が必要であるにもかかわらず，量子シミュレーションは量子コンピュータの重要な応用になりそうである．量子システムのシミュレーションは多くの分野で重要な問題である．とりわけ量子化学では古典コンピュータの計算上の制約により，多くの重要なバイオシステムで生じる大規模分子は言うに及ばず，中規模サイズの分子の振る舞いですら正確なシミュレーションが困難である．したがって，このようなシステムをより速くより正確にシミュレートできれば，量子現象が重要な役割を果たす他の分野の進展を可能にするという歓迎すべき効果をもたらす．

将来量子コンピュータでも効率良くシミュレートできない，自然界の物理現象が見出されるかも知れない．これは悪いニュースではなく素晴らしいことである！少なくともそれに刺激されて，我々は計算モデルを拡張して新しい現象を取り込むであろうし，計算モデルの能力が現状以上に向上するであろう．そのような現象に付随して，非常に興味ある物理効果が見出されることもあり得る！

量子シミュレーションのもう1つの応用は，他の量子アルゴリズムに対する見通しを得る一般的方法として使うことである．例えば，量子探索アルゴリズムを量子シミュレーション問題の解法と見なす方法を6.2節（第II巻）で説明する．このようなアプローチにより，量子探索アルゴリズムの起源をより容易に理解できる．

最後に量子シミュレーションはMooreの法則に関して興味ある楽天的な「量子的な系 (corollary)」を与える．Mooreの法則が述べるところはコストが一定のとき古典コンピュータの能力は2年程度で2倍になるということを思い出そう．しかし我々は今古典コンピュータ上で量子システムのシミュレーションを行っており，シミュレート対象に1個のqビット（またはそれ以上のシステム）を追加したいとする．これにより量子システムの状態の記述を記憶するためには古典コンピュータに2倍かそれ以上のメモリが必要となり，ダイナミックスをシミュレートするには同様かそれ以上の時間的コストが必要になる．こう考えると次のようなMooreの法則に関する量子的な系が導かれる．量子コンピュータに2年毎に**1個のqビット**が追加されるならば，量子コンピュータの発展は古典コンピュータのペースを守れるであろう．量子コンピュータの利点の性格がまだ明確ではないので，この系はあまり真剣に考えるようなものではない．とはいってもこの発見的見解によって量子コンピュータに興味を持つ理由と，いつの日か少なくとも幾つかの応用において最強の古典コンピュータを凌ぐという希望を読者に伝える役に立つであろう．

量子計算の能力

量子コンピュータはどれほど強力なのか？何がその能力の原因であろうか？古典コンピュータより量子コンピュータが強力であることを強く示唆する，素因数分解のような例によって感触が育まれつつあるけれども，これらの疑問に対する

答えはまだわからない．それでも量子コンピュータ上で効率良く解ける問題はすべて古典コンピュータでも効率良く解けるという意味で，量子コンピュータが古典コンピュータ以上に強力でない可能性がまだ残っている．他方で最終的には量子コンピュータが古典コンピュータよりもはるかに強力になるかも知れない．ここでは量子計算の能力についてわかっていることを手短に見てみよう．

計算量理論 (computational complexity theory) は古典的か量子的かを問わず，各種の計算問題の困難さを分類することを主題とする．量子コンピュータの能力を理解するためにまず計算量の一般的概念を調べて見る．最も基本的な概念は**計算量クラス** (complexity class) である．計算量のクラスとは問題を解くに必要な計算リソースに関する特徴を一定とする条件下で，計算問題を集めたものと考えてよい．[2]

最も重要な計算量クラスは **P**，**NP** という名前で呼ばれている．大雑把にいえば **P** は古典コンピュータで素早く解ける計算問題のクラスである．**NP** は古典コンピュータ上で素早くチェックできる解を持つ問題のクラスである．**P** と **NP** の違いを理解するために，整数 n の素因数を見付ける問題を考える．これまでよく知られているようにこの問題を古典コンピュータで高速に解く方法はなく，この問題が **P** にないことを示唆している．他方で誰かがある数 p が n の因数であることを教えてくれれば，n を p で整除することによってこれが正しいかどうか容易にチェックできるので，素因数分解は **NP** の問題である．

問題を解く能力は可能な解をチェックする能力をも意味するので明らかに **P** は **NP** の部分集合である．**NP** の中で **P** でない問題があるかどうかは明らかでない．多分コンピュータ科学の理論で最も重要な未解決の問題は，この2つのクラスが異なるかどうかを決定することである：

---

[2]訳注：本書に現れる計算量クラスの略号は次の意味を持つ．分類と名称は，例えば Scott Aarronson: The Complexity Zoo, http://www.complexityzoo.com/ に詳しい．
BPP: Bounded-error probalistic polynomial-time
BQP: Bounded-erroe quantum polynomial-time
coNP: Complement of NP
EXP: Exponential time
L: Logarithmic space
MAXSNP: Maximization strict NP
NP: Nondeterministic polynomial-time
NPI: NP intermediate
P: Polynomial-time
PSPACE: Polynomial-space

$$\mathbf{P} \overset{?}{\neq} \mathbf{NP}. \tag{1.55}$$

多くの研究者は**NP**の中には**P**でない問題が含まれると信じている．特に**NP**問題には重要な部分クラスである**NP**完全問題が存在しており，これは2つの意味で極めて重要である．第1に**NP**完全であることがわかっている何千ものしかも高度に重要な問題が存在すること．第2にどの**NP**完全問題も**NP**の他のすべての問題とある意味で「少なくとも同じくらい困難」である．もっと正確に言えば特定の**NP**完全問題を解くアルゴリズムは，わずかな負担増で**NP**における他の任意の問題を解くのに使うことができる．特にもし**P**$\neq$ **NP**ならば，如何なる**NP**完全問題も古典コンピュータで効率良く解けないことになる．

量子コンピュータで幾つかの問題 — 素因数分解のような問題 — が解けるのは事実であるが，量子コンピュータを使って**NP**の問題を高速で解くことができるかどうかはわかっていない．多くの人たちは素因数分解が**NP**問題ではあるが**P**の問題ではないと信じている．（なお素因数分解は**NP**完全とは考えられていない．もし**NP**完全ならば，量子コンピュータを用いてすべての**NP**問題を効率的に解く方法がすでにわかっているはずである．）すべての**NP**問題を量子コンピュータで効率良く解けるならば，確かに興奮すべきことである．**NP**のすべての問題を解くために量子並列性の変形を使うことはできない，という非常に興味ある否定的結果が知られている．特に**NP**問題を量子コンピュータで解くという問題への1つのアプローチは，問題のすべての可能な解を並列に探索する何らかの形の量子並列性を用いることである．このような探索ベースの方法論では，すべての**NP**問題に対する効率的な解は生まれないことを6.6節（第II巻）で示す．このアプローチが失敗するのは残念であるが，**NP**問題に何か奥深い構造が存在して，それを使って量子コンピュータですべての**NP**問題を効率的に解くことができる可能性を排除するものではない．

Pと**NP**は沢山の定義された計算量クラスのほんの2つである．もう1つの重要な計算量のクラスは**PSPACE**である．大雑把に言えば**PSPACE**は空間的サイズが小さい（つまりコンピュータが「小さい」）が，時間的には必ずしも小さくはない（つまり「長い」計算ができる），計算リソースを用いて解くことができる問題より成っている．**PSPACE**は**P**と**NP**の両方より断然大きいと信じられているが，これも証明はされていない．最後に計算量のクラス**BPP**は解の誤

り確率の上限が（例えば1/4に）与えられたときに，確率的アルゴリズムを用いて多項式時間で解ける問題のクラスである．**BPP**は古典コンピュータ上で，**P**よりも効率良く解ける問題のクラスであると広く見なされている．**P**のほうが深く研究されているので，ここでは**BPP**よりも**P**に着目することとしたが，**BPP**についても同様の概念と結論を導くことができる．

量子計算量のクラスはどうか？ 我々は**BQP**が有界の誤り確率が許される場合に，量子コンピュータ上で効率良く解けるすべての計算問題のクラスであると定義する．（厳密には**BQP**の定義によれば，**BQP**は古典計算量のクラスの**P**よりも**BPP**に類似しているが，ここの議論ではこの微妙な差は無視して**P**と類似しているとして扱う．）**BQP**が**P**，**NP**および**PSPACE**とどう対応するかは正確にはわかっていない．わかっていることは量子コンピュータはすべての**P**の問題を効率良く解けることと，**PSPACE**外の問題は効率良く解けないことである．したがって，図1.21に示したように**BQP**は**P**と**PSPACE**のどこか間にある．重要な意味はもし量子コンピュータが古典コンピュータよりも厳密に能力が高いことが証明されるならば，**P**は**PSPACE**と等しくないことになる．この証明は多くのコンピュータ科学者が試みたが成功していない．このことは量子コンピュータが古典コンピュータよりも強力であると証明することは — この主張に有利な証拠は沢山あるが — 大いに意味がある可能性を示唆している．

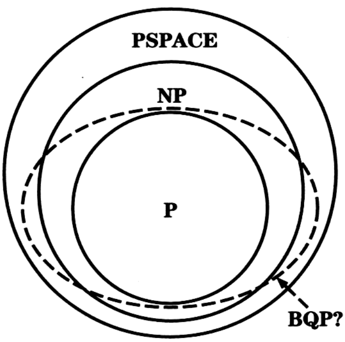


図 1.21: 古典的および量子的計算量クラスの関係．量子コンピュータは**P**の任意の問題を高速で解くことができるが，**PSPACE**の外の問題は高速で解けないことが知られている．量子コンピュータが**P**と**PSPACE**の間のどの辺に位置するかはわかっていない．そもそも**PSPACE**が**P**より大きいかさえわかっていないのが一因である．

ここでは量子コンピュータの究極の能力についてこれ以上推測を重ねることは

差し控えて，第 II 部（第 II 巻）の大部分を占める話題である高速量子アルゴリズムの原理がもっと理解されるまで待つことにする．すでに明らかになったように，量子計算の**理論**は計算に関する伝統的理解に対する重要で興味ある挑戦である．これが重要な挑戦である理由は，量子計算の理論モデルは我々の知る限り「自然」の振る舞いとつじつまが合っているので，**実験的**に実現可能だからである．もしそうでなければ量子計算は 1 つの数学的興味に終わってしまう．

1.5 量子情報処理の実験

量子計算と量子情報は素晴らしい理論の発見であるが，重ね合せやもつれといったその核心となる概念は，我々の周囲の日常世界から得られる直観と相反するものである．これらの概念が本当に自然界の動きを記述するというどんな証拠があるのか？ 大規模量子コンピュータの実現は実験的に可能か？ もしかして大規模化を阻む何か本質的な物理学的原理があるのではないか？ 次の 2 節で我々はこの疑問に取り組む．最初は自然界に q ビットが存在する証拠を示した有名な Stern-Gerlach の実験である．次に視野を広げて如何にして現実的な量子情報処理システムを構築するかという幅広い問題を取り扱う．

1.5.1 Stern-Gerlach の実験

q ビットは量子計算と量子情報の基本要素である．q ビットの性質を備えたシステムが自然界に存在するかはどうすればわかるのか？ 本書の執筆時点でこれを示す膨大な証拠が存在するが，量子力学の初期の時点では q ビットの構造は明らかでなく，現在我々が q ビットという言葉で理解している現象 — 2 準位量子システム — を前に人々は格闘していた．

q ビットの構造を示す初期の決定的な（そして非常に有名な）実験は 1921 年に Stern によって考案され，1922 年にフランクフルトで Gerlach によって実行された．Stern-Gerlach の最初の実験では図 1.22 に示すように高温炉から出た熱い原子「ビーム」が磁界で偏向され各原子の到達位置が記録される．最初の実験では銀原子が使われたが，構造が複雑で我々が議論しているような効果は明瞭に現れなかったので，1927 年に行われた水素原子を使った実験に沿って説明する．

観測された基本的効果は同じであるが，水素原子のほうが議論しやすいからである．しかし 1920 年代の人達にはこのような特権は与えられておらず，彼らは観察したもっと複雑な効果を説明するために，創意ある思考を巡らせなければならなかったことを心に留めておいて欲しい．

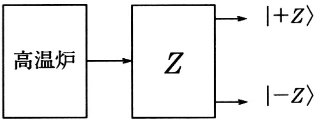


図 1.22: Stern-Gerlach の実験の模式図．高温炉で形成された熱い水素原子ビームが磁界中を通ると，上向き $|+Z\rangle$ または下向き $|-Z\rangle$ に偏向される．

水素原子は陽子と軌道運動をする電子から成る．この電子は陽子の周りを回る小さな「電流」と考えてよい．この電流によって原子に磁界が発生し各原子は物理学者が呼ぶ「磁気双極子」を持つ．その結果，各原子は電子の回転軸方向を向いた小さな棒磁石のような振る舞いをする．小さな棒磁石を磁界中に投げ入れると磁石は磁場によって曲げられる．Stern-Gerlach の実験における原子にも同様な偏向が起きると予想された．

原子がどれくらい曲げられるかは原子の磁気双極子モーメント— 電子が回転する軸 — と Stern-Gerlach の装置が作り出す磁界に依存する．詳細に立ち入ることは避けるが Stern-Gerlach の装置を適切に作ると，磁気双極子モーメントの $\hat{z}$ 成分 — $\hat{z}$ はある固定した外部の軸方向 — に依存した角度だけ原子を曲げることができる．

この実験が行われたときに 2 つの大きな驚きがあった．1 つは高温炉で作られる熱い原子は当然ランダムにあらゆる方向を向いた双極子を持っているので，Stern-Gerlach の装置を出た原子はすべての角度に連続に分布するはずである．しかし実際の観察では原子の出射角度は**離散的**な集合であった．物理学者は原子の磁気双極子モーメントが量子化されている — 何かある基本量の整数倍になる — と仮定してこの現象を説明することができた．

Stern-Gerlach の実験における量子化の観察は 1920 年代の物理学者にとって驚くべきことではあったが，当時他のシステムにおいて量子化効果が知られるようになっていたので，それ自体が全くの驚きというわけではなかった．本当に驚きであったのはこの実験で観察されたピークの**数**である．実験に使われた水素原子

の磁気双極子モーメントはゼロのはずである．古典的にこれは電子の軌道運動がないことに対応するので，これ自体驚くべきことであるが，当時の量子力学で知られていたところでは容認できる考えであった．これによれば水素原子の磁気モーメントはゼロになるはずなので，原子ビームの方向は一本だけであってこのビームが磁界で偏向されるはずがないのである．にもかかわらず2つの偏向ビームが観察され，磁界で一方が上向きに，他方が下向きに偏向されたのである！

この困ったビーム偏向はかなりの努力の末に，水素原子中の電子には**スピン**と呼ぶ量を伴うという考えが提唱されて説明された．このスピンは陽子の周りを回る電子の通常の回転運動に伴うものではなく，電子に付随する全く新しい量である．偉大な物理学者である Heisenberg はこの考えが示されたときに，それを「勇敢 (brave)」と呼んだ．本質的に新しい物理量を自然界に導入したという意味で実際この考えは勇敢な概念であった．電子スピンは電子の回転運動による寄与と並んで，水素原子の磁気双極子モーメントに対する**もう1つの**寄与をなすものとされている．

電子スピンを適切に記述するにはどうすればよいか？ 1つの推測としてスピンは単一ビットで規定され水素原子の偏向が上向きか下向きかを規定するものと考えるかも知れない．もう1つの実験をしてみると，この考えに修正や変更が必要かどうかを決めるのに役立つ情報が得られる．Stern-Gerlach の元の実験装置を図 1.22 に表す．この出力は2本の原子ビームであり $|+Z\rangle$ と $|-Z\rangle$ と呼ぶことにする．（量子力学風の記号を使っているが，もちろん他のどんな記号を好きに使っても構わない.） 図 1.23 に示すように2つの Stern-Gerlach 装置を縦続に接続するとする．2番目の装置を**横向きに傾けて**原子が磁界により $\hat{x}$ 軸方向に偏向するようにする．この思考実験では1番目の Stern-Gerlach 装置の出力から $|-Z\rangle$ ビームを遮り，$\hat{x}$ 軸方向を向いた2番目の装置に送り込む．最終出力での検出器は $\hat{x}$ 軸方向に沿った分布を測定する．

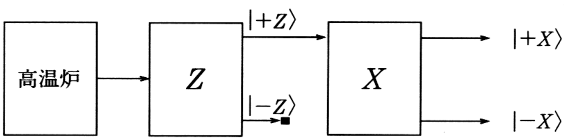


図 1.23: 縦続型の Stern-Gerlach 測定.

$+\hat{z}$ 方向を向いた古典的磁気双極子は $\hat{x}$ 方向に正味の磁気モーメントを持たないので，最終的出力は中央の（無偏向）ピークだけであると考えるかも知れない．しかし実験では等強度の2つの偏向ピークが現れる！ 多分これらの原子が異常であり，各々の軸に沿って独立に確定した磁気モーメントを持っているのかも知れない．つまり観察される2つのスピン量を表すには，2番目の装置を通過する各原子は多分 $|+Z\rangle|+X\rangle$ または $|+Z\rangle|-X\rangle$ とでも書ける状態にあると記述できるのかも知れない．

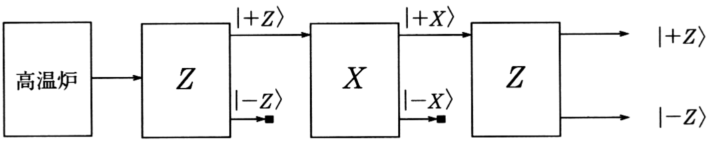


図 1.24: 3段縦続型の Stern-Gerlach 測定．

図1.24に示したもう1つの実験では前の装置の出力ビームの一方を，$\hat{z}$ 方向を向いた2つ目の Stern-Gerlach 装置に通すことにより，この仮説を検証できる．もし原子が $|+Z\rangle$ 方向を向いているならば出力ピークは $|+Z\rangle$ の1つだけである．しかしここでも最終出力に **2つの**ビームが観察される．したがって，結論は古典的な期待とは一見異なって $|+Z\rangle$ 状態は等しい割合の状態 $|+X\rangle$ と $|-X\rangle$ から成っており，$|+X\rangle$ 状態は等しい割合の状態 $|+Z\rangle$ と $|-Z\rangle$ より成っている．もしも Stern-Gerlach 装置が $\hat{y}$ のような何か他の軸方向に向けられても，同様な結論に達するであろう．

この実験で観察された振る舞いは q ビットモデルで簡単に説明される．1つの q ビットの状態を $|0\rangle$ と $|1\rangle$ とし，他の状態を次のように指定する．

$$|+Z\rangle \leftarrow |0\rangle \tag{1.56}$$

$$|-Z\rangle \leftarrow |1\rangle \tag{1.57}$$

$$|+X\rangle \leftarrow (|0\rangle + |1\rangle)/\sqrt{2} \tag{1.58}$$

$$|-X\rangle \leftarrow (|0\rangle - |1\rangle)/\sqrt{2} \tag{1.59}$$

そのうえで $\hat{z}$ 方向の Stern-Gerlach 装置が計算基底 $|0\rangle$，$|1\rangle$ でスピン（すなわち，q ビット）を測定し，$\hat{x}$ 方向の Stern-Gerlach 装置が基底 $(|0\rangle + |1\rangle)/\sqrt{2}$, $(|0\rangle - |1\rangle)/\sqrt{2}$ に関してスピンを測定すると仮定すると，縦続型の Stern-Gerlach

実験の結果を説明することができる．例えば，$\hat{z}-\hat{x}-\hat{z}$ の縦続型実験において最初の Stern-Gerlach 装置の出力スピン状態が $|+Z\rangle = |0\rangle = (|+X\rangle + |-X\rangle)/\sqrt{2}$ であると仮定すると，第 2 の装置の出力で $|+X\rangle$ を得る確率は 1/2，$|-X\rangle$ を得る確率は 1/2 である．同様に 3 番目の装置から $|+Z\rangle$ を得る確率は 1/2 である．したがって，q ビットモデルによってこの縦続型の Stern-Gerlach 実験の結果を予測できるのである．

この例は q ビットが自然界のシステムをモデル化する際の信頼すべき方法であることを示している．もちろん電子スピンを理解する正確な方法であること以上のすべての疑問を解決するものではなく，もっと多くの実験的確証が必要である．それにもかかわらずこのような実験が多くあるので，現在我々は電子スピンは q ビットモデルで最もよく記述できると信じている．さらにそれ以上に q ビットモデル（およびその高次元への拡張，つまり量子力学）によって**あらゆる**物理システムを記述することができる．次にどのようなシステムが量子情報処理に特に適しているか，という疑問に目を向ける．

1.5.2　現実的な量子情報処理の展望

量子情報処理デバイスを構築することは第 3 千年紀の科学技術者にとって大きな挑戦である．我々はこの挑戦に対処できるであろうか？ そもそも可能性はあるのか？ 試みる価値はあるのか？ もしそうなら如何にすれば達成できるのか？ これらは本書全体に及ぶ困難ではあるが重要な疑問であるが，この項で手短な答えを試みてみよう．

最も基本的疑問は，何らかの形で量子情報処理の妨げになる何か原理上の問題はないか？ということである．2 つの障害の可能性が思い当たる．1 つは雑音によって有用な量子情報処理に本質的な障害が起きるかも知れない．もう 1 つは量子力学が正しくないかも知れない．

雑音が実用的量子情報処理デバイスを開発する際の重要な障害であることに疑いはない．それは大規模量子情報処理デバイスの開発を永遠に阻む**基本的に除き得ない**障害ではないのか？ 量子誤り訂正符号理論が強く示唆するところによれば，量子雑音は対処すべき具体的問題ではあるが，**原理**上の基本的障害を提示するものではない．具体的には量子計算にはしきい**値定理**があり，大雑把にいえば

量子コンピュータ内の雑音レベルをある一定の「しきい値」以下に抑えられれば，量子誤り訂正符号を用いて計算量をあまり犠牲にすることなく誤りを本質的に無限に (ad infinitum) 低く抑えることができる．しきい値定理には量子コンピュータで生じる雑音の性質と大きさ，および量子計算に利用できるアーキテクチャに関して広い仮定が設けられている．しかしこれらの仮定が満たされれば，量子情報処理に対する雑音の影響は本質的に無視できる．8章，10章，12章（第III巻）において量子雑音，量子誤り訂正およびしきい値定理について詳しく議論する．

量子情報処理を排除するかも知れない第2の可能性は量子力学が正しくないかも知れないということである．実際（相対論的および非相対論的）量子力学の妥当性を厳密に検証することは量子情報処理デバイスの構築に関心を持つ1つの理由である．大規模量子システム全体を完全に制御するという自然界の領域はこれまで探索されておらず，量子力学によって適切に説明されていない領域において，おそらく自然は何か新たな驚きを見せるであろう．このようなことが起きれば科学史における重大な発見になるであろうし，量子力学が行ったのと同様に，他の科学技術分野に対してかなり重要な影響を及ぼすと期待される．そのような発見は量子計算と量子情報にもインパクトを与えるかも知れないが，そのインパクトによって量子情報処理能力が強化されるか，弱体化するか，それとも影響を受けないかは前もって予測できない．そのような効果が見出されるまで，また見出されなければこれらが情報処理に影響を与えるかどうか知る由もないので，現在得られている根拠に則って，本書では量子力学が完全であり世界を正しく記述すると仮定する．

量子情報処理デバイスを構築する基本的障害がないとして，なぜ膨大な時間と資金のリソースを投入して，その構築をはかるのか？ そうしたい理由については幾つか理由をあげてすでに議論してきた．つまり，量子暗号や大きな合成数の素因数分解のような実用的応用と，自然界と情報処理に対する基本的洞察を得ることである．

これらは素晴らしい理由であり，相当の時間と資金の投資を正当化するものである．しかし公平を期すならば，量子情報処理と古典情報処理の相対的利点を追求するには，両者の相対的計算能力をより明確に描く必要がある．そのような描像を得るには量子計算と量子情報の基礎に関するさらなる理論研究が必要である．特に興味があるのは「量子コンピュータは古典コンピュータよりも強力か？」とい

う疑問に対する確定的答えである．そのような質問に対する答えが当面得られないとしても，量子情報処理の実験的実現を目指す研究者の手助けとなるために，いろいろな計算量レベルにおける，興味ある応用への進路を明確にしておくことは有用である．歴史的に見ても長期の目的に至る踏み台として，短期ないし中期の目標を示すことにより技術の進歩がしばしば促進されてきた．マイクロプロセッサが最初はエレベータやその他の簡単なデバイスの制御装置に使われ，その後パーソナルコンピュータの基本素子として使われるようになったことを考えて欲しい(その先どうなるかは誰にもわからない)．大規模量子情報処理の長期ゴールを達成することに関心を寄せる人達のために，短期および中期の目標に至る道筋を以下にスケッチしてみる．

小規模ならば驚くほど多数の量子計算と量子情報の応用が知られている．これらすべてがその従弟分に当たる量子素因数分解アルゴリズムほど華々しくはないが，小規模応用に使うのは比較的容易なので，それ自身中期的目標として非常に重要である．

量子状態トモグラフィーと量子プロセストモグラフィーは，それ自体興味深い対象であると同時に，量子計算と量子情報にとって非常に重要な基本プロセスである．量子状態トモグラフィーはシステムの量子状態を決定する方法である．これを行うには同じ量子状態を繰り返し生成し，量子状態を完全に記述するために異なる方法で測定することによって量子状態の「隠れた」性質— これは測定によって状態を直接決められないことを思い出して欲しい — を克服する必要がある．量子プロセストモグラフィーは（これと深く関連しているが）もっと野心的な手続きであり，量子状態の**ダイナミックス**を完全に解明するものである．例えば，量子プロセストモグラフィーは量子ゲートや量子通信チャンネルの性能を解明したり，システムの異なる雑音過程のタイプや大きさを決定するのに用いられる．量子計算と量子情報への自明な応用はさておき，量子プロセストモグラフィーは量子効果が重要な働きをする如何なる科学技術分野においても，基本操作の評価・改善を助ける診断ツールとして重要な応用があると期待されている．量子状態トモグラフィーと量子プロセストモグラフィーは 8 章（第 III 巻）において詳しく述べる．

いろいろな小規模な通信の基本要素も非常に興味深い．量子暗号と量子テレポーテーションについてはすでに述べた．前者は高度な安全性が要求される少量の鍵

情報配信を含む具体的応用において有用である．量子テレポーテーションの実用はおそらく未解決の問題である．12 章 (第 III 巻) において量子テレポーテーションが雑音が存在するときネットワーク上の遠隔ノード間で，量子状態を伝送するための極めて有用な基本過程になることを示す．通信したいノード間に EPR 対を配送することに努力を集中するという発想である．通信途中で EPR 対がこわれるかも知れないが，そのときには特別の「もつれの抽出」(entanglement distillation) プロトコルを用いて EPR 対を「純粋化」(clean up) し，ある場所から別の場所へ量子状態をテレポートするのに使えるようにする．実際雑音フリーの q ビット通信を可能にする従来の量子誤り訂正技術よりも優れた性能が，もつれの抽出とテレポーテーションを基にしたプロトコルによって提供できる．

中規模応用についてはどうか？ 有望な量子情報処理の中規模の応用として量子システムのシミュレーションがある．数十個の「q ビット」を含む量子システム（または同等の他の基本システム）をシミュレートするのは，最大級のスーパコンピュータの計算リソースにとっても負担が大きい．50 個の q ビットを含むシステムがあるとしよう．このようなシステムを記述するには $2^{50} \approx 10^{15}$ 個の複素振幅を必要とする．もし振幅を 128 ビット精度で記憶するとすれば，各振幅の記憶に 256 ビットつまり 32 バイト，全体で 32×10^{15} バイトの情報つまり 32,000 テラバイトの情報を記憶しなければならない．これは現存コンピュータの全容量を優に超えており，Moore の法則が予定通り続くとして，21 世紀の 2 番目の 10 年間に現れるスーパコンピュータの記憶容量に匹敵する．同じ精度で 90 個の q ビットを扱うには 32×10^{27} バイトが必要になり，これを 1 ビット当たり 1 原子で表すとキログラム（またはそれ以上）の物質に相当する．

量子シミュレーションはどれくらい有用であろうか？ 化学結合の強さや分光特性のような材料の基本的特性を決定するには，従来方法がまだ使われるように思われる．しかし基本的性質が理解されると，新たな分子の性質を設計・試験する研究ツールとして，量子シミュレーションが大いに有用になると考えられる．従来の研究室設備には広範囲の分子設計をテストするために，多くの異なる「ハードウェア」 — 化学薬品や試験設備等々 — を必要とした．これら多くのハードウェアは量子コンピュータ上ですべてソフトウェアでシミュレートされ，経済化と高速化がはかられる．もちろん最終設計と試験は実際の物理的システムを用いて行わねばならないが，量子コンピュータはより良い最終結果に至る途中で，探

求・評価すべき設計の可能性を広げる役割を果たすであろう．古典コンピュータにおいて，新分子の設計法として**先験的** (ab initio) 手法が試みられてきたが，量子力学のシミュレーションに必要な膨大な計算リソースが古典コンピュータ上で制約されるために，あまり成功していない．量子コンピュータならば比較的近い将来より良い成果があげられるであろう．

大規模応用についてはどうか？ 量子シミュレーションや量子暗号のような応用の大規模化はさておくと，大規模な応用はあまり知られていない．大きな整数の素因数分解，離散対数の計算，量子探索等である．最初の 2 つに関する関心は主として現行公開鍵暗号システムの能力を制限するという**否定的**効果により生じている．（それらの問題それ自身に興味を持つ数学者にも現実的な興味を引き起こすかも知れない.）素因数分解や離散対数が長期にわたって重要な応用のすべてを占めるとは思えない．発見的探索手法は広く使われるので量子探索は非常に有用であり，6 章（第 II 巻）において応用の可能性を議論する．実際に素晴らしいのはもっと多くの量子情報処理の大規模応用があることである．これこそ将来の大きなゴールである！

量子情報処理に向けた潜在的応用の道筋が示されたとして，現実の物理システムでそれを如何に達成するか？ すでに数個の q ビットを用いた幾つかの小規模な量子情報処理デバイスに関する現実的提案がある．多分最も実現しやすいのは**光技術**つまり電磁波に基づくものであろう．反射鏡やビームスプリッタのような単純なデバイスを用いて光子の基本的な操作ができる．興味深いことに困難な点は要求に応じて単一光子を発生することであった．その代わりに実験家達は単一光子を「ときどき」ランダムに発生させ，それが起きるのを待つ方法を選んだ．量子暗号，超高密度符号化および量子テレポーテーションはそのような光技術を用いて実現された．光技術の最大の利点は光子が量子力学的情報の非常に安定な運び手であることである．欠点のほうは光子が互いに直接相互作用をしないことである．その代わりに相互作用は原子のように何か他のものを介して行われなければならず，そのため実験に付加的な雑音や複雑さが入ってくる．2 光子間の**実効的**相互作用は本質的に 2 つのステップで行われる．つまり第 1 光子が原子と相互作用をし，次にその原子が第 2 光子と相互作用をすることによって，全体として 2 光子間の相互作用が生じる．

別の方法は異なるタイプの原子の閉じ込めに基づくものである．限られた空間

内に少数の帯電した原子を閉じ込める**イオントラップ**と，帯電していない原子を閉じ込める**中性原子トラップ**がある．原子トラップに基礎をおく量子情報処理では原子を用いて情報を蓄積する．この方法には電磁波も際だった働きをするが，「光学的」量子情報処理と呼ぶアプローチとは少し異なる役割を果たす．これらの方法では光子に情報を蓄えるのではなく，原子それ自身に蓄えられた情報を操作するのに光子を使う．個別の原子にパルス電磁波を照射することにより，単一 q ビットゲートの動作を行わせる．隣接原子は（例えば）双極子相互作用を通じて，互いに影響し合い量子ゲート作用を行う．さらに実験家は適切な電磁波パルスを原子に加えて隣接原子間の相互作用の性質を厳密に変化させて，システム中のどのゲートを作用させるかを制御できる．最後に量子計算に使う計算基底の超精密測定を実現する技術には，確立されて久しい**量子ジャンプ** (quantum jump) を用いてこれらシステムの量子測定を行う．

量子情報処理のもう 1 つ別の方法は NMR の略称で知られている**核磁気共鳴** (nuclear mgnetic resonace) に基づく方法である．この方法では量子情報情報を分子内原子の**核スピン**に蓄え電磁波でその情報を操作する．この方法には固有の困難さがあり，NMR では個別原子核に直接アクセスすることができない．その代わりに膨大な数（通常およそ 10^{15} 個）の本質的に同一な分子が溶液中に蓄えられている．試料に電磁波パルスを照射して各分子にほぼ同様の応答をさせる．各分子が独立なコンピュータであると考えたほうがよく，試料は膨大な数の（古典的）並列動作をするコンピュータを含んでいる．NMR 量子情報処理では他の量子情報処理方法と異なり 3 つの困難に直面する．第 1 は分子は室温で平衡状態を保っており，その温度は典型的スピン反転温度よりも高いのでスピンはほとんど完全にランダムな向きを向いている．このため量子情報処理用として初期状態の「雑音」が大きい．この雑音抑制は興味ある話題であり 7 章（第 II 巻）で述べる．第 2 の問題は NMR に適用できる測定は量子情報処理で行いたい一般的測定として不十分なことである．にもかかわらず多くの量子情報処理の例では NMR で可能な測定で十分である．第 3 に NMR では各分子個別に処理をすることはできないのに，どうすれば個別 q ビットを適切に操作できるのか疑問に思うであろう．幸いなことに分子内の異なる原子核は異なる性質を持っているので個別にアドレスできる ― あるいは少なくとも量子計算に重要な演算をするに十分な微細スケールでアドレスできる．

大規模量子計算処理を行うに必要な多くの要素も提案されている．イオントラップ中の少数 q ビットで行われる状態生成と測定，NMR を用いて少数分子で実現される処理機能，固体システムの作成技術を用いた超大規模化の可能性等である．これらの全要素を兼ね備えた単一システムを実現するには，夢の量子コンピュータに向けた長い道程をたどらねばならない．不幸にしてこれらのシステムは非常に異なっていて多種類にわたるので，大規模量子コンピュータを手にするには何年もかかるであろう．しかし（異なるとはいえ）実現されているシステムでこれらすべての性質がすでに存在していることは，長期的に見て大規模量子情報処理が実現される良い前兆といえる．そのうえにこれは 2 つあるいはそれ以上の既存技術の最良の性質を組み合わせると，**ハイブリッド**設計を追求する利点が大きいことを示唆している．例えば，**電磁波共振器** (electromagnetic cavity) 中に原子をトラップすることを目指して多くの研究が行われている．これによれば共振器内の原子を光技術で柔軟に操作して，従来の原子トラップではできなかった単一原子の実時間フィードバック制御が可能になる．

結論として量子情報処理を単なるもう 1 つの情報処理とは考えないことが重要である．例えば量子計算を — 1980 年代初期に次世代メモリの有力候補と褒めちぎられた「バブルメモリ」をはじめ多くの他の熱狂が消え去ったように — コンピュータの進展途上に出現し時間と共に消え去っていく一時的な技術の熱狂の 1 つとして簡単に片づけがちである．量子計算は多くの**異なる**実現形態を持ち得る情報処理の**抽象的パラダイム**なので，この見方は誤っている．量子計算の 2 つの異なる提案を技術的利点の上で比較するときに，「良い」提案と「悪い」提案を比較するのは意味があるが，量子コンピュータに関する貧弱な提案であっても古典コンピュータの見事な設計とは異なる性質のものである．

1.6 量子情報

量子計算と量子情報の世界で「量子情報」という言葉は 2 つの異なる使い方がされる．第 1 は量子力学を用いた情報処理に関するものと解釈される演算操作すべてを包括的に指す．この用法では量子計算，量子テレポーテーション，非クローン化定理，その他事実上本書の全トピックスを含む．

「量子情報」の第 2 の用法はもっと専門的なものであり，「基本的」な量子情

報処理タスク に関する研究を指す．例えば特定の詳細な量子アルゴリズムは「基本」の範囲外なので，量子アルゴリズムの設計はこれには含まれない．混乱を避けるために対応する古典的分野を記述するのによく使われている「(古典) 情報理論」と並行して，この特定の分野を指すときには「量子情報理論」という言葉を使うことにする．もちろん「量子情報理論」という言葉はそれ自身で支障をきたすことがある — 理論的考察だけが重要であるように見られかねない！ もちろんそのようなことはなく量子情報理論によって研究される基本プロセスの実験的検証にも大いに興味がある．

本節の目的は量子情報理論の基本概念の紹介である．基礎的な量子情報処理タスクに話を限っても，一見何の関連もない主題が「量子情報理論」の題目に含まれるので，量子情報理論は初心者にとって混乱した動物園のように見えるかも知れない．ある部分はテーマがまだ発展途上にあり，断片がどう組み合わされるのかわかっていないためである．しかし量子情報理論の研究を統合する二三の基本的ゴールを示すことはできる：

(1) **量子力学における基本的な静的リソースのクラスを解明する．** 一例をあげるとqビット，別の例は ビットである．古典物理学は量子物理学の特別な場合なので，古典情報理論に現れる基本的な静的リソースが量子情報理論でも大いに関連しても不思議はない．基本的な静的リソースについてもう1つ例をあげれば，遠く離れた2人の当事者に共有されたBell状態である．

(2) **量子力学における基本的な動的プロセスのクラスを解明する．** 簡単な例はある時間量子状態を蓄えておく**メモリ**である．自明でないプロセスをあげれば，2人の当事者AliceとBob間の量子情報伝送，量子情報状態のコピー(もしくはコピーの試み)，雑音から量子情報を保護するプロセス等がある．

(3) **基本的な動的プロセスを行う際に必要なリソース配分を定量化する．** 例えば，2人の当事者間で雑音のある通信チャンネルを用いて信頼度良く量子情報を伝送するに必要な最少のリソースは何か？

同様のゴールは古典情報理論でも設定できる．しかし量子情報理論は，その静的および動的要素が元来古典情報理論の全要素をも含んでいるので，量子情報理論の範囲のほうが古典情報理論より広い．

この節では量子情報理論で研究される幾例かの疑問について述べ，対象とする基本的な静的・動的要素および考えるべきリソースのトレードオフを明らかにす

る．最初は古典情報理論家にとって馴染み深い，量子チャンネルを使って古典情報を送る問題を例にとって始める．次にこれを発展させて，量子力学に存在する幾つかの新しい静的および動的プロセス — 量子誤り訂正，量子状態の識別問題およびもつれの変換等 — を追求する．章の最後に量子情報のツールを量子計算と量子情報以外に応用する波及効果について述べる．

1.6.1 量子情報処理： 例題

量子チャンネルによる古典情報の伝送

古典情報理論の基本的成果は Shannon の**雑音のないチャンネルにおける符号化定理** (noiseless channel coding theorem) と**雑音のあるチャンネルにおける符号化定理** (noisy channel coding theorem) である．雑音のないチャンネルでの符号化定理は情報源から発信された情報を蓄積するのに何ビットが必要かを定量化しており，雑音のあるチャンネルでの符号化定理は雑音のある通信チャンネルを通してどれだけの情報を信頼度良く伝送できるかを定量化している．

情報源 (information source) とは何を意味するか？ この意味を定義することは古典情報理論と量子情報理論の基本的問題であり，今後何度か調べ直すことになる．当面暫定的定義として，古典情報源は確率集合 p_j, $j = 1, 2, \ldots, d$ で記述されるものとしておく．情報源を使う度ごとに独立に確率 p_j でランダムに選ばれた「文字」(letter) j が発信される．例えば情報源が英語の文章ならば数 j はアルファベットと句読点の文字に相当し，確率 p_j は通常の英文に現れる文字の相対頻度で与えられる．英文の文字が前後の文字とは独立に現れるというのは正しくないが，我々の目的には十分良い近似である．

通常の英文にはかなりの冗長性が含まれており，この冗長性を利用して文章を**圧縮** (compress) できる．例えば通常の英文には文字「e」が「z」より頻繁に現れる．英文をうまく圧縮するには，文字「z」を表す情報ビットよりも少ないビット数で文字「e」を表すのがよい．Shannon の雑音のないチャンネルでの符号化定理は，まさにこのような圧縮法が如何にうまく働くかを規定している．正確に言えば雑音のないチャンネルにおける符号化定理の教えるところによれば，確率 p_j で記述される古典情報源は，各回平均した利用情報のビット数が $H(p_j)$ となるように圧縮できる．ここで $H(p_j) \equiv -\sum_j p_j \log p_j$ は情報源の確率分布の関数で

あり **Shannon のエントロピー** (Shannon entropy) と呼ぶ．さらに雑音のないチャンネルでの符号化定理は，これより少ないビット数で情報源を表すと圧縮情報を回復したときに誤り確率が高くなることを示している．(雑音のないチャンネルでの Shannon の符号化定理は 12 章（第 III 巻）で詳しく扱う．)

Shannon の雑音のないチャンネルでの符号化定理は，先に示した情報理論の全ゴールが達成された良い例である．2 つの静的リソース— ビットと情報源 — が解明され（ゴール 1)，1 段階の動的プロセス— 情報源の圧縮と原情報を回復する解凍 — が解明された（ゴール 2)．最後に消費された情報を決める量的な判断基準— 最適のデータ圧縮法 — が見出された（ゴール 3)．

Shannon の第 2 の偉大な成果である雑音のあるチャンネルでの符号化定理は雑音があるチャンネルを通して信頼性良く伝送できる情報量を定量的に規定している．ある情報源の情報を雑音のあるチャンネルを通じて他の場所に伝送したいとする．その場所が宇宙の別の場所にあるか，あるいは別の時間に届けるとする — 後者は雑音があるときの情報蓄積という問題になる．2 つの例の意図は誤り訂正符号を用いて情報を符号化すると，チャンネルで生じた雑音は受信端で修正できることにある．誤り訂正符号がこれを行う方法は，チャンネルを通じて送るべき情報にあらかじめ冗長性を与えておき，情報のある部分が壊れても元の情報が回復できるようにする．例えば単一ビットを送るチャンネルに雑音があり，情報源の各ビットを信頼性良く送るのにあらかじめ 2 ビットを使って符号化しなければならないほど雑音が大きいとする．チャンネルを 1 回使って送れるのはおおまかに言って 1/2 ビットの情報であるから，このようなチャンネルの**容量**は 1/2 ビットであるという．Shannon の雑音のあるチャンネルでの符号化定理は，任意の雑音のあるチャンネルの容量を求める一般的手続きを提供する．

Shannon の雑音のあるチャンネルの符号化定理もまた，先に述べた情報理論の 3 つのゴールを達成している．2 つの静的リソース — 情報源とチャンネルを通じて送られるビット — が含まれている（ゴール 1)．3 つの動的プロセスが含まれている（ゴール 2)．第 1 のプロセスはチャンネルの雑音である．この雑音を除去するために誤り訂正符号による符号化と復号化という対になるプロセスを実行する．雑音が一定だと信頼性の良い情報伝送を行うには，最適の誤り訂正手法でどれだけの冗長性を導入すればいいかを Shannon の定理は教えてくれる（ゴール 3)．

雑音のないチャンネルとあるチャンネルの符号化定理に対して，Shannon は古典的システムの情報源からの出力 — ビットとそれに類するもの — を蓄積するという制約を課した．量子情報理論における当然の質問は，蓄積媒体が変化して古典情報が量子状態を媒体として伝送されるとどうなるかということである．例えば Alice がある情報源で作られた古典情報を圧縮し，圧縮情報を Bob に伝送して Bob は圧縮を解くとする．圧縮情報を蓄積するのに用いる媒質が量子状態ならば，Shannon の雑音のないチャンネルの符号化定理を使って最適な圧縮・解凍法を決定することはできない．仮に q ビットを使って古典的場合より良く圧縮できるとすれば驚くべきことである．12 章（第 III 巻）でこの疑問について調べ，実際には q ビットを使っても雑音のないチャンネルで情報を伝送するに要する通信量は節約されないことを証明する．

当然次のステップは**雑音のある**量子チャンネルを通して古典情報を伝送する問題を調べることである．理想的に我々が望むものは，情報伝送におけるそのようなチャンネルの**容量** (capacity) を定量化することである．容量を求めることは幾つかの理由で手際を要する仕事である．雑音は連続空間で起きるため量子力学では種々の雑音モードが生じ，雑音の抑制に古典的誤り訂正技術がどう役立つか全く明らかでない．例えば仮に**もつれ状態** (entangled state) を用いて古典情報を符号化して，次に雑音のあるチャンネルを通して一度に 1 つずつ伝送するのが有利なのか？ あるいは多分もつれの測定を用いて復号化するのが有利なのか？ 12 章（第 III 巻）で我々は **HSW 定理** (Holevo-Schumacher-Westmoreland theorem) を証明する．この定理はそのようなチャンネル容量の下界を与える．実際 HSW 定理は完全な証明はまだ知られていないが，容量を正確に評価すると広く信じられている！ 残る問題はもつれ状態を用いた符号化により，HSW 定理で示される下界以上に容量が高められるかどうかである．今日得られている証拠によればこれによって容量は上がらないが，この推論の正否を決めることは量子情報理論の興味深い未解決の問題である．

量子チャンネルによる量子情報の伝送

もとより古典情報は量子力学で得られる唯一の静的リソースではない．量子状態それ自身が当然 — 古典情報より自然な — 静的リソースである．Shannon の符

号化定理と別の量子版 — ここでは量子状態の圧縮と解凍を含む — を見てみる．

はじめに古典情報源の定義と同様に，情報源の量子的概念を幾つか定義する必要がある．古典的場合と同様にこれにも幾つもの方法があるが，明確さを優先して量子情報源は確率 p_j の集合と，それに対応する量子状態 $|\psi_j\rangle$ で記述できるという定義を暫定的に採用する．情報源の情報を1回使う度に確率 p_j で状態 $|\psi_j\rangle$ が作り出され，異なる回の情報は互いに独立であるとする．

そのような量子力学的情報源の出力を圧縮することはできるか？ 確率 p で状態 $|0\rangle$，確率 $1-p$ で状態 $|1\rangle$ を出力するqビット情報源を考える．これは単一ビット — 確率 p で0，確率 $1-p$ で1のいずれか — を出力する古典情報源と本質的に同じであり，したがって驚くまでもなく情報源を圧縮するのに同じテクニックが使えて，圧縮した情報を蓄積するには $H(p,1-p)$ 個のqビットしか必要としない．ここで $H(\cdot)$ はShannonのエントロピー関数である．

これに代わってもしも情報源が確率 p で状態 $|0\rangle$，確率 $1-p$ で状態 $(|0\rangle+|1\rangle)/\sqrt{2}$ を出力するとすればどうなるか？ 我々は一般に状態 $|0\rangle$ と $(|0\rangle+|1\rangle)/\sqrt{2}$ を完全には区別できないので，古典的な標準手法を用いることはできない．この場合にも何らかの圧縮が可能であろうか？

この例でもある種の圧縮を施すことが可能なことがわかっている．興味深いことには圧縮はもはや**誤りフリー**とはならず，情報源で作られた量子状態は圧縮・解凍過程で少し歪むかも知れない．にもかかわらずこの歪みは非常に小さく，情報源出力が十分大きいブロックで圧縮される極限では歪みは無視できる．歪みを定量化するために圧縮方法に対して**忠実度** (fidelity) の尺度を導入し，圧縮によって導入された平均的歪みを測定する．量子データ圧縮の理想は圧縮されたデータが非常に良い忠実度で回復することである．忠実度とは解凍を正確に行う確率に似たものと考えてよい — ブロック長が十分長い極限ではこれが誤り0の極限である1に近づく．

Schumacherの雑音のないチャンネルの符号化定理 (Schumacher's noiseless channnel coding theorem) は1に近い忠実度で回復できるという制約下で，量子データ圧縮を行うために要求される情報源を定量化する．発生確率が p の直交量子状態 $|\psi\rangle$ を発生する情報源の場合に，Schumacherの定理は情報源を古典的限界 $H(p_j)$ まで圧縮できるが，それを越えることはないと教えている．Schumacherの定理は情報源が一般的な非直交状態の場合にも，量子情報源をどれだけ圧縮で

きるか答えることができて，その答えは Shannon のエントロピー $H(p_j)$ ではない！ エントロピーに似た新たな量である **von Neumann のエントロピー** (von Neumann entropy) が正しい答えである．一般に von Neumann のエントロピーは状態 $|\psi_j\rangle$ が直交するとき，かつそのときにのみ Shannon のエントロピーと一致する．そうでなければ情報源 p_j，$|\psi_j\rangle$ に対する von Neumann のエントロピーは一般に Shannon のエントロピー $H(p_j)$ より厳密に小さい．したがって，例えば確率 p で状態 $|0\rangle$，確率 $1-p$ で状態 $(|0\rangle+|1\rangle)/\sqrt{2}$ を発生する情報源は使用回数 1 回当たり $H(p,1-p)$ より少ない q ビットを用いて信頼度良く圧縮ができる！

このリソース節約の理由は直観的に容易に理解できる．状態 $|0\rangle$ を確率 p で，状態 $(|0\rangle+|1\rangle)/\sqrt{2}$ を確率 $1-p$ で出力する情報源を多数 n 回使うと考える．大数の法則により，高い確率で情報源は $|0\rangle$ を np 回，$(|0\rangle+|1\rangle)/\sqrt{2}$ を $n(1-p)$ 回出力する．つまり含まれるシステムの並べ替えを除くと出力は,

$$|0\rangle^{\otimes np}\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n(1-p)}, \tag{1.60}$$

右側因子 $|0\rangle+|1\rangle$ の積を展開する．$n(1-p)$ は大きいので再び大数の法則を用いて，この積はおよそ半分が $|0\rangle$ 半分が $|1\rangle$ と見積もられる．つまり $|0\rangle+|1\rangle$ の積は次の重ね合せで近似される：

$$|0\rangle^{\otimes n(1-p)/2}|1\rangle^{\otimes n(1-p)/2}. \tag{1.61}$$

したがって，情報源の出力状態は次の形の項の重ね合せで近似できる：

$$|0\rangle^{\otimes n(1+p)/2}|1\rangle^{\otimes n(1-p)/2}. \tag{1.62}$$

この形の状態が幾つあるか？ およそ n 個が $n(1+p)/2$ を選ぶので，Stirling の近似式よりこの数は $N\equiv 2^{nH[(1+p)/2,(1-p)/2]}$ に等しい．単純な圧縮方法では式 (1.62) の形の全状態に $|c_1\rangle$ から $|c_N\rangle$ までのラベルを付ける．情報源から出力された n 個の q ビットをユニタリー変換により $|c_j\rangle$ は $|j\rangle|0\rangle^{\otimes n-nH[(1+p)/2,(1-p)/2]}$ に変換することができる．ここで j は $nH[(1+p)/2,(1-p)/2]$ 個のビット番号である．圧縮操作ではこのユニタリー変換を行った後，$n-nH[(1+p)/2,(1-p)/2]$ 個の最終 q ビットを削除して， $nH[(1+p)/2,(1-p)/2]$ 個の q ビット圧縮状

態を残す．解凍には圧縮状態に状態 $|0\rangle^{\otimes n-nH[(1+p)/2,(1-p)/2]}$ を付加してユニタリー逆変換を行う．

この量子データ圧縮・解凍を行うには情報源を1回使う毎に $H[(1+p)/2,(1-p)/2]$ 個のqビットを蓄える必要があり，$p \geq 1/3$ である限りShannonの雑音のない符号化定理から単純に期待されるqビット数 $H(p,1-p)$ 個より改善される．実際には12章（第III巻）で示すようにSchumacherの雑音のないチャンネルの符号化定理によればもう少し良い性能が許容される．しかしその改善の本質的理由はここで圧縮を行ったのと同じ理由である．つまりここでは $|0\rangle$ と $(|0\rangle+|1\rangle)/\sqrt{2}$ が直交していないことを利用した．直観的にこれら状態は両方とも $|0\rangle$ 方向成分を持つので冗長性があり，直交状態に比べて物理的類似性が高い．今述べた符号化において我々が利用したのはこの冗長性であり，Schumacherの雑音のないチャンネルの符号化定理を完全に証明する際にも使われる．$p \geq 1/3$ の制約が生じるのは，もし $p < 1/3$ ならこの特定の方法では状態の冗長性が利用できなくなるからである．問題中に含まれる冗長性を有効的に**増加させる**ことによって目的を達成しているのである！ もちろんこれは我々が選んだ特定の人為的例であり一般の解法ではデータ圧縮の達成により適した方法で冗長性を利用する．

Schumacherの雑音のないチャンネルの符号化定理は，量子状態の圧縮・解凍を対象として，Shannonの雑音のないチャンネルの符号化定理を相似的に発展させた理論である．ではShannonnの雑音のあるチャンネルの符号化定理に類似の理論を見出すことができるか？ 量子誤り訂正符号の理論を用いてこの重要な疑問に関してかなりの進展が見られている．しかし完全に満足できる類似の理論はまだ見付かっていない．量子チャンネル容量に関してわかっている事柄を12章（第III巻）で解説する．

量子識別性

これまで我々が考えてきたすべての動的プロセス — 圧縮，解凍，雑音，誤り訂正符号化，復号化 — は古典情報理論と量子情報理論の両方で起こるものであった．しかし，量子状態のような新しい形の情報が導入されると，古典情報理論で考えた以上に動的プロセスのクラスが拡大する．その良い例が量子状態の識別である．古典的には少なくとも原理上異なる情報の項目は識別できることに慣れて

きた．もちろん文字「a」がにじむと「o」と実際上非常に識別しづらいことがあるが，原理上2つの可能性は確実に識別可能である．

他方量子力学で任意の状態を識別することは必ずしも**可能でない**．例えば状態 $|0\rangle$ と $(|0\rangle + |1\rangle)/\sqrt{2}$ を高い信頼度で識別する量子力学的プロセスは許されていない．この厳密な証明には我々が今持っていないツールを使うが（2章で行う），これができないことは例を使ってかなり容易に納得できる．例えば2つの状態を計算基底で測定して識別を試みる．状態 $|0\rangle$ が与えられたときは測定により確率1で0が得られる．しかし $(|0\rangle + |1\rangle)/\sqrt{2}$ を測定すると確率1/2で0，確率1/2で1を得る．したがって，測定結果が1ならば $|0\rangle$ はあり得ないので，その状態は $(|0\rangle + |1\rangle)/\sqrt{2}$ であることがわかるが，測定結果が0ならば量子状態の特定に関して如何なる推論もできない．

非直交状態を識別できないことが量子計算と量子情報の核心にある．量子状態が測定にかからない隠れた情報を持ち，それが量子アルゴリズムと量子暗号の鍵となる役割を果たす，というのが我々の主張の要点である．量子情報理論の1つの中心的課題は，非直交量子状態をうまく識別できる尺度を見付けることであり，9章と12章（第III巻）の多くはこのゴールに関係している．この概論では識別不能性の興味ある側面を2つ指摘するに留める．それは光速より速い通信と「量子通貨」への応用である．

取りあえず任意の量子状態を識別できると想定する．これはもつれを用いて光速より速い通信の可能性を意味することを示す．Alice と Bob は状態 $(|00\rangle + |11\rangle)/\sqrt{2}$ にある q ビットのもつれ対を共有するとする．このときもし Alice が計算基底で測定すると測定後の状態は確率1/2で $|00\rangle$，確率1/2で $|11\rangle$ となる．したがって，Bob の状態は確率1/2で $|0\rangle$，確率1/2で $|1\rangle$ のいずれかになる．しかしこれに代わって Alice が基底 $|+\rangle$, $|-\rangle$ で測定するとする．ここで $|0\rangle = (|+\rangle + |-\rangle)/\sqrt{2}$, $|1\rangle = (|+\rangle - |-\rangle)/\sqrt{2}$ である．簡単な代数計算により Alice と Bob の初期状態は $(|++\rangle + |--\rangle)/\sqrt{2}$ と書ける．したがって，もし Alice が基底 $|+\rangle$, $|-\rangle$ で測定すれば，測定後の Bob のシステムの状態はそれぞれ確率1/2で $|+\rangle$ または $|-\rangle$ となる．以上はすべて基礎的量子力学である．しかしもしも Bob が4つの状態 $|0\rangle$, $|1\rangle$, $|+\rangle$, $|-\rangle$ を互いに識別できるデバイスを持っていてそれを使うとすると，彼には Alice が計算基底を使ったかそれとも $|+\rangle$, $|-\rangle$ 基底を使ったかがわかる．さらに Alice が測定をするとすぐに Bob は瞬

時にその情報を手に入れる．この結果 Alice と Bob は光速より速い通信を行ったことになる！ もちろん我々は非直交量子状態を識別できないことを知っており，この制約が物理世界が従うべき他の性質と密接に結合していることをこの例は示している．

非直交量子状態の識別不能性は必ずしもハンディキャップにはならない．それは利益をもたらすこともある．銀行が（古典的な）通し番号と状態 $|0\rangle$ または $(|0\rangle+|1\rangle)/\sqrt{2}$ にある一連の q ビットを付けた紙幣を発行するとする．これら埋め込まれた 2 つの状態の順序は銀行以外誰も知らず，通し番号と埋め込まれた状態の対応リストは銀行が管理しているとする．偽造志願者が元の紙幣の q ビット状態を確定すると壊れてしまうのでこの紙幣を正確に偽造することは不可能である．紙幣が提示されると（認証のうまい）商人は銀行に連絡して通し番号を告げ，紙幣に埋め込んだ一連の状態番号を聞くことによって偽造紙幣でないことが確認できる．彼らは銀行の指示に基づいて q ビットを基底 $|0\rangle$, $|1\rangle$ または $(|0\rangle+|1\rangle)/\sqrt{2}$，$(|0\rangle-|1\rangle)/\sqrt{2}$ で測定し紙幣が真正であるかチェックする．チェックする q ビット数が増えると指数関数的に偽造検出確率が増加するので，この段階ですべての偽札作りが検出できる！ このアイディアは他の多くの量子暗号プロトコルの基本となっており，非直交量子状態の識別不能性が有効であることを示している．

演習 1.2: 2 つの非直交量子状態 $|\psi\rangle$ または $|\varphi\rangle$ の一方を入力すると状態を正しく見分けるデバイスがもしあれば，それを使って非クローン化定理に逆らって状態 $|\psi\rangle$ と $|\varphi\rangle$ のクローンが作れることを説明せよ．逆にクローン作成デバイスがあると，それは非直交量子状態の識別に使えることを説明せよ．

もつれの生成と変換

もつれは量子力学の基本的な静的リソースの 1 つである．その性質は古典情報理論でよく知っているリソースと驚くほど異なっており，まだ十分理解されていない．我々にできるのはもつれに関する成果の不完全なコラージュを作るのが精々である．その解を理解するに必要なすべての言葉がまだそろっているわけではないが，もつれに関連した 2 つの情報理論的問題を見てみよう．

もつれの生成 (creating entanglement) は量子情報理論において興味ある単純な動的プロセスである．2 人の当事者があらかじめもつれ状態を共有していない

として，共有するべき特定のもつれ状態を作り出すには，幾つのqビットを互いに交換する必要があるか？ 2番目の興味ある動的プロセスは，ある形から別の形への**もつれの変換** (transforming entanglement) である．例えば，Alice と Bob が Bell 状態を互いに共有しており，何か他の形のもつれ状態に変換したいとする．この仕事をするにはどんなリソースが必要か？ 互いに通信しなくてもできるか？古典通信だけでよいか？ 量子通信が必要ならばどれくらいの通信量か？

これらを始めとするもつれの生成・変換に関するもっと複雑な疑問に答えることは，それ自身魅力ある研究領域であると同時に，それにより量子計算のようなタスクへの見通しを約束する．例えば，分散量子計算は単に2人またはそれ以上の当事者間でもつれ状態を作り出す方法と見なしてもよい．分散量子計算等を行うのに必要な通信量の下界は適切なもつれ状態を作り出すのに必要な通信量の下界から導かれる．

1.6.2 広義の量子情報

量子情報理論のほんの一部を概観してきた．第 III 部（第 III 巻）で量子情報理論について詳しく議論する．特に 11 章で量子および古典情報理論におけるエントロピーの基本的性質を扱い，12 章では純粋な量子情報理論に焦点を絞る．

量子情報理論は量子計算と量子情報の中で最も抽象的部分であり，ある意味で最も基礎的部分でもある．量子情報理論や究極的に量子計算と量子情報のすべてを駆り立てる疑問は，**何が量子情報処理を可能ならしめるか？**という疑問である．量子論的世界と古典論的世界を隔てるものは何か？ 古典的世界で得られなかったどんなリソースを量子計算に使うことができるか？ これらの疑問に対して現在得られる答えは立ちこめた霧の中にある不完全なものである．我々の希望は今後霧が晴れて量子情報処理の可能性と限界を評価して明らかにすることである．

問題 1.1: **（Feynman と Gates の会話）** 計算の将来に関して現在の時点で Bill Gates と Richard Feynman が友好的な議論を行うと想定して，その内容を 2000 語程度にまとめよ．（コメント：この質問に答えるのは本書の残りの部分を読んだ後のほうがよいかも知れない．1つの可能な答えは次の「歴史と参考資料」欄を参照.）

問題 1.2:　量子計算と量子情報においてこれまでになされた最も意義深い発見は何か？ 教養のある非専門家の読者を対象にその発見について 2000 語程度で小論文を書け．（コメント：前の質問と同様にこの質問に答えるのは本書の残りの部分を読んだ後のほうがよいかも知れない．）

歴史と参考資料

本章の大部分の内容は以後の章でもっと詳しく述べる．したがって，ここで示す歴史的資料と参考資料は後の章で繰り返されないものに限る．

量子計算と量子情報が発展してきた歴史的経緯をつなぎ合わせるには，多くの分野の歴史を広く見渡す必要がある．本章ではこの歴史をつなぎ合わせる試みをしてきたが，頁数と能力の限界のためやむなく多くの内容を省かざるを得なかった．次に推奨する資料でこの不足が少しでも取り戻せればありがたい．

量子力学の歴史は多くの場所で語られてきた．我々は特に卓越した Pais の著書 [Pai82] [Pai86] [Pai91] を推薦する．これら 3 つのうちで [Pai86] が最も直接的に量子力学の発展に関係している．しかし Pais による Einstein[Pai82] と Bohr[Pai91] の伝記も少し少ないが興味ある内容を含んでいる．量子力学に基づく技術の進歩は Milburn によって述べられた [Mil97] [Mil98]．コンピュータ科学の基礎に関する Turing の素晴らしい論文 [Tur36] は一読の価値がある．それは Davis の価値ある歴史的論文集で見ることができる [Dav65]．Hofstadter[Hof79] と Penrose[Pen89] にはコンピュータ科学に関する興味深く有益な議論が述べられている．Shasha と Lazere による 15 人の指導的コンピュータ科学者の伝記 [SL98] はコンピュータ科学の歴史における多くの異なる側面に対して洞察力を与えてくれる．最後に Knuth の印象的な書物 [Knu97] [Knu98a] [Knu98b] は驚くべき量の歴史上の情報を提供する．情報理論の基礎を作った Shannon の輝かしい論文 [Sha48] は優れた読み物である（[SW49] にも掲載されている）．MacWilliams と Sloane[MS77] は誤り訂正符号の優れた教科書であるだけでなく，膨大な量の有益な歴史上の情報を含んでいる．同様に Cover と Thomas[CT91] は情報理論に優れた教科書であり広範囲にわたる歴史上の情報を含んでいる．Shannon の論文集は多くの有用な歴史的事項と合わせて Sloane と Wyner が編集した大部な書物に収められている [SW93]．Slepian[Sle74] にも情報理論の有益な論文が集められて

いる．暗号は古くからある技術であり複雑でしばしば興味深い歴史を持っている．Kahn[Kah96] の書は暗号の膨大な歴史であり豊富な情報を備えている．最近の発展に関しては Menezas, van Oorschot, Vanstone[MvOV96]，Schneier[Sch96a]，Diffie と Landau[DL98] の本を推薦する．

量子テレポーテーションは Bennett, Brassard, Crépeau, Jozsa, Peres, Wootters[BBC+93] によって発見され，その後いろいろな異なる形で実験的に実現された．Boschi, Branca, De Martini, Hardy, Popescu[BBM+98] は光技術を用いて，Bouwmeester, Pan, Mattle, Eibl, Weinfurter, Zeilinger [BPM+97] は光子の偏光を用いて，Furusawa, Sørensen, Braunstein, Fuchs, Kimble, Polzik [FSB+98] は光の「スクイーズ」状態を用いて，Nielsen, Knill, Laflamme [NKL98] は NMR を用いてそれぞれ実験を行った．

Deutsch の問題は Deutsch [Deu85] によって提出され，同じ論文で 1 ビット解が示された．一般の n ビットへの拡張は Deutsch と Jozsa[DJ92] により行われた．これら初期の論文のアルゴリズムはその後 Cleve，Ekert，Macchiavello，Mosca [CEMM98] と Tapp の未発表論文で独立に実質的に改良された．本章では改良されたアルゴリズムについて述べた．これは隠れ部分群の枠組みによく適合するものであり 5 章（第 II 巻）でまた議論する．Deutsch の元のアルゴリズムは確率的なものであり Deutsch と Jozsa はこれを決定性アルゴリズムに改良した．しかし彼らの方法には本章で示した改良版とは異なり 2 つの関数の評価を必要とする．それにもかかわらずこれらのアルゴリズムを Deutch のアルゴリズム，Deutsch-Jozsa のアルゴリズムと呼ぶのが慣例である．これは 2 つの偉大な進展をたたえるものであり Deutsch は量子コンピュータが古典コンピュータよりも速い計算ができることを具体的に示し，Deutsch と Jozsa は問題を解くに必要な時間スケールに同様のギャップがあることを初めて示してこれを拡張した．

Stern-Gerlach の実験は Sakurai[Sak95]，Feynman, Leighton, Sands の第 III 巻 [FLS65a] や Cohen-Tannoudji, Diu, Laloë [CTDL77a] [CTDL77b] のような標準的教科書に優れた議論が見られる．

問題 1.1 は Rahim[Rah99] の愉快な記事に示唆されたものである．

第2章　量子力学入門

俺は物理学者じゃないが，何が大切かくらいはわかっているさ．
— 船乗り Popye

量子力学：まさに黒魔術の計算．　— Albert Einstein

量子力学は我々が知る世界を最も正確に，かつ最も完全に記述する．それは量子計算と量子情報を理解するための基礎でもある．本章は量子計算と量子情報を完全に理解するのに必要な，量子力学の基礎知識のすべてを提供する．量子力学に関する予備知識は前提としていない．

量子力学が難しい学問だという世評があるが，実は学ぶのは簡単である．この世評は複雑な分子の構造を理解するというような，幾つかの応用が難しいことに由来する．しかしこれらの応用は量子力学を修得するための基本ではないので，我々はそのような応用についての議論はしない．量子力学を理解するのに前もって必要とするものは，初歩的な線形代数に親しんでいることくらいである．この知識さえあれば量子力学の予備知識がなくとも数時間で，簡単な問題が解けるようになる．

すでに量子力学を熟知している読者は，我々が使う慣用記号（大部分は標準的であるが）に親しみ，すべての内容を知っていることを確認するために，本章をざっと読むだけでよい．予備知識があまりないかあるいは全くない読者は本章を熟読し，演習も解いてみるべきである．演習を解くのが難しければ，まず先に進んで後でまた戻ってもう一度試みればよい．

本章は 2.1 節の線形代数に関する復習から始まる．この節では初歩的な線形代数の知識を仮定しているが，物理学者が量子力学を記述するのに使う記号を — 多

くの線形代数の入門書とは異なっているので — 紹介する．2.2 節では量子力学の基本公理について述べる．この節が済めば読者は量子力学の**すべての**基本原理を理解したことになる．この節には内容の理解を深める手助けに，多くの簡単な演習が用意されている．この章の残りと次章以降では基本的に新たな物理学の原理を導入することなく，この内容を元にして説明を行う．2.3 節では**超高密度符号化** (superdense coding) について説明する．これには単純な構成の中に多くの量子力学公理が組み合わされており，驚くべきかつ啓発的な量子情報処理の実例である．2.4 節と 2.5 節では強力な数学ツール — **密度オペレータ** (density operator), **純粋化** (purification), **Schmidt 分解** (Schmidt decomposition) — を示す．これらは量子計算と量子情報の研究にとりわけ有用である．これらのツールを理解することは基礎的な量子力学の理解を深めることにつながる．最後に 2.6 節で如何に量子力学が「古典的」世界像の理解を超えるかという疑問を検証する．

2.1　線形代数

> この本は教えるためと同じくらい，悩ませ当惑させるために書かれた．
> — 「About Vectors」の第 1 行，Banesh Hoffmann
>
> 人生は複雑 (複素数，complex) である—それには現実 (実数部，real part) と想像 (虚数部，imaginary part) がある．
> — 作者未詳

線形代数はベクトル空間と，そこにおける線形演算の学問である．初歩的線形代数をしっかり把握すると量子力学がよく理解できる．本節では線形代数の基本概念を概観し，量子力学においてこれらの概念を表す標準的な表記法について述べる．これらの表記法は図 2.1 において量子力学での表記法を左欄に，それに対する線形代数の説明を右欄にまとめてある．この表を見て右欄の概念の幾つかに見覚えがあるかを確認するとよい．

我々の意見では量子力学の公理の理解を阻む主な要因は公理それ自体にあるのではなく，それを理解するのに必要な線形代数の表記法の多さにある．物理学者が量子力学に用いている見慣れない Dirac の表記法と相まって，それは（間違って）とても恐ろしい印象を与える．これらの理由で量子力学に精通していない読

者には，以降の内容は手早く読み通して，主として使われている記号の基礎を理解することに注力することを勧める．そして本章のメイントピックス — 量子力学の公理 — を注意深く学び，必要に応じて線形代数の概念と表記法を学ぶために戻ってくればよい．

線形代数の基礎となる対象は**ベクトル空間** (vector space) である．我々に最も関係があるベクトル空間は n 個の複素数の組 $(z_1, \ldots, z_n)$(n-tuple) のすべてを要素とする空間 $\mathbf{C}^n$ である．ベクトル空間の要素を**ベクトル** (vector) と呼び，ベクトルを表すのに次のような列の行列表記を用いる．

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \tag{2.1}$$

和演算 (addition operation) は 2 つのベクトルの組を 1 つのベクトルに変換する演算として定義する．$\mathbf{C}^n$ 空間ではベクトルの和演算は次式で定義する．

$$\begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} + \begin{bmatrix} z_1' \\ \vdots \\ z_n' \end{bmatrix} \equiv \begin{bmatrix} z_1 + z_1' \\ \vdots \\ z_n + z_n' \end{bmatrix}, \tag{2.2}$$

ここで右辺にある足し算は通常の複素数の和である．さらにベクトル空間には**スカラー倍**演算 (multiplication by a scalar operation) もある．$\mathbf{C}^n$ 空間ではこの演算は次式で定義される．

$$z \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix} \equiv \begin{bmatrix} zz_1 \\ \vdots \\ zz_n \end{bmatrix}, \tag{2.3}$$

ただし z は**スカラー** (scalar) つまり複素数であり，右辺の積は通常の複素数の積である．物理学者は複素数のことを c ナンバー (c-number) と呼ぶことがある．

我々は量子力学のために線形代数を学んでいるので，線形代数の概念を表すには量子力学で用いる標準的な慣用記号を用いる．ベクトル空間におけるベクトルを量子力学的な慣用記号で表すと

$$|\psi\rangle \tag{2.4}$$

となる．ψ はベクトルに対するラベルである（どんなラベルでもよいが我々は ψ や φ のような簡単なラベルを使う）．$|\cdot\rangle$ はそれがベクトルであることを示す記号である．$|\psi\rangle$ 全体を**ケット** (ket) と呼ぶことがあるが，ここではあまり使わない．

ベクトル空間には**ゼロベクトル** (zero vector) と呼ぶ特別なベクトルが含まれており，それを 0 で表す．ゼロベクトルは任意のベクトル $|v\rangle$ に対して $|v\rangle+0=|v\rangle$ が成り立つ．我々はゼロベクトルに対してケット記号を用いないことに注意する．これは唯一の例外であり，この例外の理由は，$|0\rangle$ は全く別のものを表すのに用いる習慣があるからである．スカラー倍演算は任意の複素数 z に対して $z0=0$ である．便宜上我々は要素 $z_1,\ldots,z_n$ を持つ列行列を表すのに記号 $(z_1,\ldots,z_n)$ を用いる．$\mathbf{C}^n$ におけるゼロベクトルは $(0,0,\ldots,0)$ である．ベクトル空間 V の**ベクトル部分空間** (vector subspace) W は V の部分集合であり，W もベクトル空間となる．つまり W はスカラーの積と和に関して閉じている．

記号	意味
z^*	複素数 z の複素共役．$(1+i)^*=1-i$
$\|\psi\rangle$	ベクトル．ケット (ket) とも呼ばれる．
$\langle\psi\|$	$\|\psi\rangle$ に双対 (dual) なベクトル．ブラ (bra) とも呼ばれる．
$\langle\varphi\|\psi\rangle$	$\|\varphi\rangle$ と $\|\psi\rangle$ の内積
$\|\varphi\rangle\otimes\|\psi\rangle$	$\|\varphi\rangle$ と $\|\psi\rangle$ のテンソル積
$\|\varphi\rangle\|\psi\rangle$	$\|\varphi\rangle$ と $\|\psi\rangle$ のテンソル積に対する簡略記号
A^*	行列 A の複素共役
A^T	行列 A の転置
$A^\dagger$	行列 A の Hermite 共役，もしくは随伴．$A^\dagger=(A^T)^*$． $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$
$\langle\varphi\|A\|\psi\rangle$	$\|\varphi\rangle$ と $A\|\psi\rangle$ の内積．$A^\dagger\|\varphi\rangle$ と $\|\psi\rangle$ の内積に等しい．

図 2.1: 線形代数の概念を表すのに量子力学で用いる標準的な慣用記号のまとめ．この記号の形は **Dirac の記号** (Dirac notation) と呼ばれる．

2.1.1　基底と線形独立

ベクトル空間の**スパン集合** (spanning set) とは，その空間の任意のベクトル $|v\rangle$ が線形結合 $|v\rangle=\sum_i a_i|v_i\rangle$ で表せるようなベクトル集合 $|v_1\rangle,\ldots,|v_n\rangle$ である．例えばベクトル空間 $\mathbf{C}^2$ のスパン集合は

$$|v_1\rangle \equiv \begin{bmatrix} 1 \\ 0 \end{bmatrix};\quad |v_2\rangle \equiv \begin{bmatrix} 0 \\ 1 \end{bmatrix} \tag{2.5}$$

という集合である．なぜなら $\mathbf{C}^2$ の任意のベクトル

$$|v\rangle = \begin{bmatrix} a_1 \\ a_2 \end{bmatrix} \tag{2.6}$$

はベクトル $|v_1\rangle$ と $|v_1\rangle$ の線形結合 $|v\rangle = a_1|v_1\rangle + a_2|v_2\rangle$ で書けるからである．ベクトル $|v_1\rangle$ と $|v_1\rangle$ はベクトル空間 $\mathbf{C}^2$ を**張る** (span) という．

一般にベクトル空間は多くの異なるスパン集合を持ち得る．例えばベクトル空間 $\mathbf{C}^2$ に対して

$$|v_1\rangle \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ 1 \end{bmatrix}; \quad |v_2\rangle \equiv \frac{1}{\sqrt{2}}\begin{bmatrix} 1 \\ -1 \end{bmatrix} \tag{2.7}$$

もスパン集合である．なぜなら任意のベクトル $|v\rangle = (a_1, a_2)$ は $|v_1\rangle$ と $|v_2\rangle$ の線形結合として書けるからである．

$$|v\rangle = \frac{a_1 + a_2}{\sqrt{2}}|v_1\rangle + \frac{a_1 - a_2}{\sqrt{2}}|v_2\rangle. \tag{2.8}$$

少なくとも 1 つの i に対して $a_i \neq 0$ であり，

$$a_1|v_1\rangle + a_2|v_2\rangle + \ldots + a_n|v_n\rangle = 0 \tag{2.9}$$

を満たす複素数の集合 $a_1, \ldots, a_n$ が存在するならば，0 でないベクトル $|v_1\rangle, \ldots, |v_n\rangle$ は**線形従属** (linearly dependent) であるという．ベクトルの集合が線形従属でなければ，それは**線形独立** (linearly independent) であるという．任意の 2 つのベクトル空間 V を張る線形独立なベクトルの集合は同じ数の要素を持つことが示せる．そのような集合を V の**基底** (basis) と呼ぶ．さらにそのような基底集合は常に存在する．基底の要素の数を V の**次元** (dimension) と定義する．本書では**有限次元** (finite dimension) のベクトル空間のみを対象とする．無限次元のベクトル空間に関連する興味深くしばしば難しい問題が多数存在する．しかし我々はそれらの問題に煩わされる必要はないであろう．

演習 2.1:（線形従属：例） $(1, -1)$, $(1, 2)$ および $(2, 1)$ は線形従属であることを示せ．

2.1.2　線形オペレータと行列

ベクトル空間 V と W の間の**線形オペレータ** (linear operetor) を入力に対して線形，すなわち

$$A\Big(\sum_i a_i|v_i\rangle\Big) = \sum_i a_i A(|v_i\rangle) \tag{2.10}$$

を満たす任意の関数 $A : V \to W$ で定義する．通常 $A(|v\rangle)$ を $A|v\rangle$ と書く．線形オペレータ A がベクトル空間 V 上で定義されている場合には，A が V から V への線形オペレータであることを意味する．**単位オペレータ** (identity operator) I_V は任意のベクトル空間 V における重要な線形オペレータであり，すべてのベクトル $|v\rangle$ に対して $I_V|v\rangle \equiv |v\rangle$ で定義する．混乱が生じないところでは下添字 V を省略して単位オペレータを単に I と書く．もう 1 つの重要な線形オペレータは**ゼロオペレータ** (zero operator) であり，0 と書く．ゼロオペレータはすべてのベクトルをゼロベクトルに移す，すなわち $0|v\rangle \equiv 0$ である．ひとたびある基底上で線形オペレータ A を規定すると，すべての入力に対する A の作用が完全に決定するのは式 (2.10) より明らかである．

V，W および X がベクトル空間であり，$A : V \to W$ と $B : W \to X$ が線形オペレータであるとする．このとき A と B との**合成** (composition) を記号 BA で表し，$(BA)(|v\rangle) \equiv B(A(|v\rangle)$ で定義する．繰り返すが $(BA)(|v\rangle)$ を省略して $BA|v\rangle$ と書く．

線形オペレータを理解する最も便利な方法は行列表現を用いることである．実際，線形オペレータによる視点と行列の視点は完全に等価であることがわかるが，行列のほうが読者に親しみがあるかも知れない．相互の関連を見るには，要素 A_{ij} をもつ $m \times n$ の複素行列 A が，行列 A と $\mathbf{C}^n$ のベクトルとの行列積により，実際にベクトル空間 $\mathbf{C}^n$ からベクトル空間 $\mathbf{C}^m$ に移す線形オペレータであることを最初に理解すると役に立つ．正確に言えば行列 A が線形オペレータであるということは

$$A\Big(\sum_i a_i|v_i\rangle\Big) = \sum_i a_i A|v_i\rangle \tag{2.11}$$

が行列 A と列ベクトルの行列積で成り立つことを意味する．明らかにこれは正しい！

行列が線形オペレータとみなせることを見た．線形オペレータを行列で表現できるか？ これから説明するように実際にこれができる．2つの視点が等価なので本書では行列理論とオペレータ理論の言葉を入れ替えて使うことがある．$A : V \to W$ がベクトル空間 V と W との間の線形オペレータであるとする．さらにV の基底が $|v_1\rangle, \ldots, |v_m\rangle$, W の基底が $|w_1\rangle, \ldots, |w_n\rangle$ であるとする．$1, \ldots, m$ の範囲の各 j に対して，

$$A|v_j\rangle = \sum_i A_{ij}|w_i\rangle \tag{2.12}$$

を満たす複素数 $A_{1j}, \ldots, A_{nj}$ が存在する．要素 A_{ij} をもつ行列 A をオペレータ A の **行列表現** (matrix representation) という．この A の行列表現はオペレータ A と完全に等価なので，今後行列表現と抽象的オペレータの視点とを互いに置き換えて使う．行列と線形オペレータを関連付けるには，線形オペレータの入力ベクトル空間の基底と出力空間の基底をを指定しなければならない．

演習 2.2:（行列表現の例） V は基底ベクトル $|0\rangle, |1\rangle$ を持つベクトル空間，A は V から V への線形オペレータ：$A|0\rangle = |1\rangle, A|1\rangle = |0\rangle$ であるとする．入力基底 $|0\rangle, |1\rangle$，出力基底 $|0\rangle, |1\rangle$ に関する A の行列表現を与えよ．A の異なる行列表現を与える入力と出力の基底を見出せ．

演習 2.3:（オペレータ積に対する行列表現） A はベクトル空間 V からベクトル空間 W への線形オペレータで，B はベクトル空間 W からベクトル空間 X への線形オペレータであるとする．$|v_i\rangle$，$|w_j\rangle$，$|x_k\rangle$ はそれぞれベクトル空間 V，W，X の基底であるとする．線形変換 BA に対する行列表現は適切な基底に関する B と A の行列表現の行列積であることを示せ．

演習 2.4:（単位元に対する行列表現） ベクトル空間 V の単位オペレータは行列表現の入出力の基底が同じであるならば，対角成分が 1 で他がすべて 0 の行列表現を持つことを示せ．この行列を**単位行列** (identity matrix) と呼ぶ．

2.1.3 Pauli の行列

我々が頻繁に使う機会がある 4 つの非常に有用な行列が **Pauli の行列** (Pauli matrix) である．これらは 2×2 の行列でありいろいろな記号で表される．行列

と対応する記号を図 2.2 に示す．Pauli の行列は量子計算と量子情報において有用なので，以後の節で登場する多くの例や演習を通じて詳しく学習し，Pauli の行列を記憶することを勧める．

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

図 2.2: Pauli の行列．I を省略して X，Y，Z だけを Pauli の行列ということがある．

2.1.4　内　積

内積 (inner product) はベクトル空間の 2 つのベクトル $|v\rangle$ と $|w\rangle$ を入力とし複素数を出力として作り出す関数である．当面は $|v\rangle$ と $|w\rangle$ の内積を $(|v\rangle, |w\rangle)$ と書くのが適切であろう．これは量子力学の標準記号ではないが本章では時によっては，$(\cdot,\cdot)$ の記号が教育のために明確に示す点で有用である．内積 $(|v\rangle, |w\rangle)$ に対する量子力学の標準的記号は $\langle v|w\rangle$ である．ここで $|v\rangle$ と $|w\rangle$ は内積空間のベクトル，記号 $\langle v|$ はベクトル $|v\rangle$ の **双対ベクトル** (dual vector) を表すのに用いられる．双対とは $\langle v|(|w\rangle) \equiv \langle v|w\rangle \equiv (|v\rangle, |w\rangle)$ で定義される内積空間 V から複素数 $\mathbf{C}$ への線形オペレータである．まもなく双対ベクトルに対する行列表現は行ベクトルであることを示す．

$V \times V$ から $\mathbf{C}$ への関数 $(\cdot,\cdot)$ が次の要請を満たすならば内積である：

(1)　$(\cdot,\cdot)$ は第 2 引数に関して線形である，すなわち

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right) = \sum_i \lambda_i (|v\rangle, |w_i\rangle). \tag{2.13}$$

(2)　$(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$

(3)　$(|v\rangle, |v\rangle) \geq 0$，等号が成り立つのは $|v\rangle = 0$ のときのみ．

例えば $\mathbf{C}^n$ には次式で定義される内積がある：

$$((y_1, \ldots, y_n), (z_1, \ldots, z_n)) \equiv \sum_i y_i^* z_i = [y_1^*, \ldots, y_n^*] \begin{bmatrix} z_1 \\ \vdots \\ z_n \end{bmatrix}. \tag{2.14}$$

内積を備えたベクトル空間を**内積空間**(inner product space) と呼ぶ.

演習 2.5: 先に定義した $(\cdot, \cdot)$ は $\mathbf{C}^n$ の内積空間であることを証明せよ.

演習 2.6: 任意の内積 $(\cdot, \cdot)$ は第 1 引数に関して共役線形であることを示せ.

$$\left(\sum_i \lambda_i |w_i\rangle, |v\rangle\right) = \sum_i \lambda_i^* (|w_i\rangle, |v\rangle). \tag{2.15}$$

量子力学の議論ではしばしば **Hilbert 空間** (Hilbert space) に触れる. 量子計算と量子情報で現れる有限次元の複素ベクトル空間において, Hilbert 空間は内積空間と**全く同じもの**である. 今後は 2 つの言葉を入れ替えて使うが, Hilbert 空間という言葉をより好んで使う. 無限次元では Hilbert 空間に内積空間よりも技術的制約が加わるが, 我々は気にすることはない.

ベクトル $|w\rangle$ と $|v\rangle$ の内積が 0 のとき両ベクトルは**直交** (orthogonal) しているという. 例えば $|w\rangle \equiv (1, 0)$ と $|v\rangle \equiv (0, 1)$ は式 (2.14) で定義した内積に関して直交している. ベクトル $|v\rangle$ の**ノルム** (norm) を次式で定義する.

$$\| |v\rangle \| \equiv \sqrt{\langle v|v\rangle}. \tag{2.16}$$

単位ベクトル (unit vector) とは, $\| |v\rangle \| = 1$ となるベクトル $|v\rangle$ である. もし $\| |v\rangle \| = 1$ ならば, $|v\rangle$ は**正規化** (規格化, normalize) されているという. 一般のベクトルをそのノルムで割ると**正規化**される. つまりゼロでない任意のベクトル $|v\rangle$ に対して $|v\rangle / \| |v\rangle \|$ は $|v\rangle$ を正規化した形である. 指数 i を持つベクトルの集合 $|i\rangle$ の各々が単位ベクトルであり, その集合のうち互いに異なるベクトルが直交しているとき, つまり指数の集合から選んだ i と j に対して $\langle i|j\rangle = \delta_{ij}$ のとき, 集合 $|i\rangle$ は**正規直交** (orthonormal) であるという.

演習 2.7: $|w\rangle \equiv (1, 1)$ および $|v\rangle \equiv (1, -1)$ が直交していることを証明せよ. これらのベクトルの正規化された形は何か？

$|w_1\rangle, \ldots, |w_d\rangle$ が内積を有するベクトル空間 V に対する基底集合であるとする．このベクトル空間に対する正規直交基底集合 $|v_1\rangle, \ldots, |v_d\rangle$ を作り出すのに使う **Gram-Schmidt の方法** (Gram-Schmidt procedure) という便利な方法がある．$|v_1\rangle \equiv |w_1\rangle/\||w_1\rangle\|$ と定義し，$1 \le k \le d-1$ に対して帰納的に $|v_{k+1}\rangle$ を次のように定義する．

$$|v_{k+1}\rangle \equiv \frac{|w_{k+1}\rangle - \sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle}{\||w_{k+1}\rangle - \sum_{i=1}^{k}\langle v_i|w_{k+1}\rangle|v_i\rangle\|}. \tag{2.17}$$

ベクトル $|v_1\rangle, \ldots, |v_d\rangle$ が正規直交集合を形成し，V の基底にもなることを示すのは難しくない．したがって，任意の（有限）d 次元のベクトル空間は正規直交基底 $|v_1\rangle, \ldots, |v_d\rangle$ を持つ．

演習 2.8: Gram-Schmidt の方法により V に対する正規直交基底が得られることを証明せよ．

これ以降線形オペレータとして行列表現を使うときには，正規直交の入出力基底に関する行列表現を意味するものとする．特に断らない限り線形オペレータの入出力空間が同一ならば，入出力基底は同一であるとする．

この約束に従うと，Hilbert 空間の内積は便利な行列表現で与えられる．$|w\rangle = \sum_i w_i|i\rangle$ と $|v\rangle = \sum_j v_j|j\rangle$ が，ベクトル $|w\rangle$ と $|v\rangle$ の正規直交基底 $|i\rangle$ による表現であるとする．このとき，$\langle i|j\rangle = \delta_{ij}$ であるから

$$\langle v|w\rangle = \left(\sum_i v_i|i\rangle, \sum_j w_j|j\rangle\right) = \sum_{ij} v_i^* w_j \delta_{ij} = \sum_i v_i^* w_i \tag{2.18}$$

$$= [v_1^* \ldots v_n^*] \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}. \tag{2.19}$$

つまり同じ正規直交基底により表現されているならば，2 つのベクトルの内積は，行列表現されたこれらベクトルのベクトル内積に等しい．ここで双対ベクトル $\langle v|$ は $|v\rangle$ の列ベクトル表現における対応成分の複素共役を成分とする行ベクトルと解釈できることがわかる．

内積を使って線形オペレータを表現する便利な方法があり，それを**外積表現** (outer product representation) と呼ぶ．$|v\rangle$ を内積空間 V のベクトル，$|w\rangle$ を内積空間 W のベクトルとする．$|w\rangle\langle v|$ は次式で定義される V から W への線形オペレータである．

$$(|w\rangle\langle v|)(|v'\rangle) \equiv |w\rangle\langle v|v'\rangle = \langle v|v'\rangle|w\rangle. \tag{2.20}$$

この式は我々の用いる記号の慣用に見事に適合しており，これによれば $|w\rangle\langle v|v'\rangle$ の表現は潜在的に次の 2 つのいずれかの意味をもつ．1 つは**オペレータ** (operator) $|w\rangle\langle v|$ が $|v'\rangle$ に働いたときの結果を表すのに用い，もう 1 つは従来の解釈通り $|w\rangle$ に複素数 $\langle v|v'\rangle$ を掛けた結果を表す．これら 2 つの潜在的な意味が同じに成るように定義を選んでいる．実際我々は後者を用いて前者を**定義**しているのである！

外積オペレータ $|w\rangle\langle v|$ の線形結合の意味は明らかである．定義により $\sum_i a_i|w_i\rangle\langle v_i|$ は $|v'\rangle$ に作用すると出力 $\sum_i a_i|w_i\rangle\langle v_i|v'\rangle$ を与える線形オペレータである．

外積表記の便利さは正規直交ベクトルに対する**完全性関係** (completenes relation) として知られる重要な結果からもわかる．$|i\rangle$ をベクトル空間 V における任意の正規直交基底とすると，任意のベクトル $|v\rangle$ はある複素数の集合 v_i を用いて $|v\rangle = \sum_i v_i|i\rangle$ と書ける．$\langle i|v\rangle = v_i$ であるから

$$\left(\sum_i |i\rangle\langle i|\right)|v\rangle = \sum_i |i\rangle\langle i|v\rangle = \sum_i v_i|i\rangle = |v\rangle. \tag{2.21}$$

最後の等号はすべての $|v\rangle$ に対して成り立つので，

$$\sum_i |i\rangle\langle i| = I \tag{2.22}$$

である．この式を**完全性関係**と呼ぶ．この 1 つの応用は外積記号で任意のオペレータを表す方法である．$A : V \to W$ を線形オペレータ，$|v_i\rangle$ を V に対する正規直交

交基底，$|w_i\rangle$ を W に対する正規直交基底とする．完全性関係を2回使うと

$$A = I_W A I_V \tag{2.23}$$
$$= \sum_{ij} |w_j\rangle\langle w_j|A|v_i\rangle\langle v_i| \tag{2.24}$$
$$= \sum_{ij} \langle w_j|A|v_i\rangle |w_j\rangle\langle v_i| \tag{2.25}$$

を得る．これは A の外積表現である．この式から入力基底 $|v_i\rangle$，出力基底 $|w_j\rangle$ に対して行列 A の i 行 j 列の行列要素は $\langle w_j|A|v_i\rangle$ で あることがわかる．

完全性関係の有用さを示す第2の応用は **Cauchy-Schwarz の不等式** (Cauchy-Schwarz inequality) である．この重要な結果はコラム 2.1 で議論する．

演習 2.9:（Pauli のオペレータと外積） Pauli の行列 (図 2.2) は2次元 Hilbert 空間に対する正規直交基底 $|0\rangle$, $|1\rangle$ に関するオペレータと考えられる．各 Pauli オペレータを外積記号で表現せよ．

演習 2.10: $|v_i\rangle$ を内積空間 V に対する正規直交基底とする．この基底 $|v_i\rangle$ に関してオペレータ $|v_j\rangle\langle v_k|$ の行列表現は何か？

コラム 2.1: Cauchy-Schwarz の不等式

Cauchy-Schwarz の不等式 (Cauchy-Schwarz inequality) は Hilbert 空間における重要な幾何学的性質である．その内容は任意の2つのベクトル $|v\rangle$，$|w\rangle$ に対して $|\langle v|w\rangle|^2 \le \langle v|v\rangle\langle w|w\rangle$ である．これを証明するには Gram-Schmidt の手続きでベクトル空間の正規直交基底 $|i\rangle$ を作り，最初の基底 $|i\rangle$ を $|w\rangle/\sqrt{\langle w|w\rangle}$ とする．完全性関係 $\sum_i |i\rangle\langle i| = I$ を用い，負でない項を落とすと目的の式を得る．

$$\langle v|v\rangle\langle w|w\rangle = \sum_i \langle v|i\rangle\langle i|v\rangle\langle w|w\rangle \tag{2.26}$$
$$\ge \frac{\langle v|w\rangle\langle w|v\rangle}{\langle w|w\rangle}\langle w|w\rangle \tag{2.27}$$
$$= \langle v|w\rangle\langle w|v\rangle = |\langle v|w\rangle|^2, \tag{2.28}$$

少し考えると等号が成り立つのは $|v\rangle$ と $|w\rangle$ が線形の関係にあるときのみ，つまり z をあるスカラーとすると $|v\rangle = z|w\rangle$ または $|w\rangle = z|v\rangle$ が成り立つときのみであることがわかる．

2.1.5 固有ベクトルと固有値

ベクトル空間における線形オペレータ A の**固有ベクトル** (eigenvector) とは $A|v\rangle = v|v\rangle$ を満たす 0 でないベクトル $|v\rangle$ である．ここで v は $|v\rangle$ に対応する A の**固有値** (eigenvalue) と呼ばれる複素数である．固有値と固有ベクトルに対するラベルとして同じ記号 v を用いるのが便利である．読者がすでに固有値と固有ベクトルの初歩的性質 —特に特性方程式を使ってこれらをどう求めるか — に慣れていると想定する．**特性関数** (characteristic function) は $c(\lambda) \equiv \det|A - \lambda I|$ で定義する．ここで det は行列の**行列式関数** (determinant function) である．特性関数はオペレータ A のみに依存し，A を表す特定の行列表現には依存しない．**特性方程式** (charecteristic equation) $c(\lambda) = 0$ の解はオペレータ A の固有値である．代数の基礎定理によるとすべての多項式は少なくとも 1 つの複素数の解を持つので，すべてのオペレータは少なくとも 1 つの固有値とそれに対応する固有ベクトルを持つ．固有値 v に対応する**固有空間** (eigenspace) とは固有値 v を持つベクトルの集合であり，A が作用するベクトル空間のベクトル部分空間になる．

ベクトル空間 V 上のオペレータに対する **対角表現** (diagonal representation) は表現 $A = \sum_i \lambda_i |i\rangle\langle i|$ である．ここでベクトル $|i\rangle$ は A の固有値 λ_i に対する固有ベクトルであり，この固有ベクトルは正規直交集合を形成する．オペレータの対角表現ができるとき，そのオペレータは**対角化可能** (diagonalizable) であるという．次項で Hilbert 空間上のオペレータが対角化できるための，簡単な必要十分条件を示す．対角表現の例として Pauli の Z 行列は次のように書ける．

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1|, \tag{2.29}$$

ここで行列表現は正規直交ベクトル $|0\rangle, |1\rangle$ に基づいている．対角表現は**正規直交**

分解 (orthonormal decomposition) と呼ぶこともある．

固有空間が1次元以上の場合，**縮退** (degenerate) しているという．例えば

$$A \equiv \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 0 \end{bmatrix} \tag{2.30}$$

で定義される行列 A は固有値2に対応して2次元の固有空間を持っている．固有ベクトル $(1,0,0)$ と $(0,1,0)$ は同じ固有値を持つ A の線形独立な固有ベクトルなので，**縮退**しているという．

演習 2.11:（Pauli の行列の固有分解） Pauli の行列 X，Y，Z の固有ベクトル，固有値および対角表現を求めよ．

演習 2.12: 次の行列は対角化できないことを証明せよ．

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{2.31}$$

2.1.6　転置共役と Hermite オペレータ

A は Hilbert 空間 V の任意の線形オペレータであるとすると，すべてのベクトル $|v\rangle$，$|w\rangle \in V$ に対して

$$(|v\rangle, A|w\rangle) = (A^\dagger|v\rangle, |w\rangle) \tag{2.32}$$

を満たす線形オペレータ $A^\dagger$ が V 上に唯1つのみ存在することがわかる．この線形オペレータをオペレータ A の**転置共役** (随伴，adjoint) または **Hermite 共役** (Hermitian conjugate) という．定義より $(AB)^\dagger = B^\dagger A^\dagger$ が容易に示せる．慣用により $|v\rangle$ がベクトルならば $|v\rangle^\dagger \equiv \langle v|$ と定義する．この定義を使えば $(A|v\rangle)^\dagger = \langle v|A^\dagger$ を示すのは難しくない．

演習 2.13: $|w\rangle$ と $|v\rangle$ が任意の2つのベクトルならば，$(|w\rangle\langle v|)^\dagger = |v\rangle\langle w|$ であることを示せ．

演習 2.14:（転置共役の反線形性） 転置共役演算は反線形 (anti-linear) であることを示せ.

$$\left(\sum_i a_i A_i\right)^\dagger = \sum_i a_i^* A_i^\dagger. \tag{2.33}$$

演習 2.15: $(A^\dagger)^\dagger = A$ であることを示せ.

オペレータ A の行列表現では，Hermite 共役演算は行列 A を共役・転置すること，すなわち $A^\dagger \equiv (A^*)^T$ である．ここで $*$ は複素共役，T は転置演算を示す．例えば

$$\begin{bmatrix} 1+3i & 2i \\ 1+i & 1-4i \end{bmatrix}^\dagger = \begin{bmatrix} 1-3i & 1-i \\ -2i & 1+4i \end{bmatrix} \tag{2.34}$$

である．

オペレータ A の転置共役が元のオペレータ A に等しいとき，そのオペレータを **Hermite オペレータ** (Hermitian) または**自己共役** (自己随伴，self-adjoint) オペレータであるという．Hermite オペレータのうち**射影オペレータ** (projector) は重要である．W が d 次元ベクトル空間 V 上の k 次元ベクトル部分空間であるとする．Gram-Schmidt の方法をを用いると，$|1\rangle, \ldots, |k\rangle$ が W の正規直交基底となるように V に対する正規直交基底 $|1\rangle, \ldots, |d\rangle$ を作ることができる．定義により

$$P \equiv \sum_{i=1}^{k} |i\rangle\langle i| \tag{2.35}$$

は部分空間 W への**射影オペレータ**である．この定義は W の正規直交基底 $|1\rangle, \ldots, |k\rangle$ と無関係であることが容易に確認できる．定義により任意のベクトル $|v\rangle$ に対して $|v\rangle\langle v|$ は Hermite オペレータである．したがって P も Hermite オペレータ，すなわち $P^\dagger = P$ である．P がそのうえで射影オペレータであるベクトル空間のことを，省略して「ベクトル空間」P と呼ぶ．P の**正規直交相補オペレータ** (orthonormal complement operator) はオペレータ $Q = I - P$ である．Q は $|k+1\rangle, \ldots, |d\rangle$ で張られたベクトル空間への射影オペレータであり，その空間を P の**正規直交相補空間** (orthonormal complement) と呼び Q と書く．

演習 2.16: 任意の射影オペレータ P は式 $P^2 = P$ を満たすことを示せ．

オペレータ A が $AA^\dagger = A^\dagger A$ を満たすとき，これを**正規** (normal) であるという．明らかに Hermite オペレータは正規である．正規オペレータに対して**スペクトル分解** (spectral decomposition) と呼ばれる注目すべき表現に関する定理がある．これによればオペレータは対角化可能であるときにのみ正規である．この結果は少し後のコラム 2.2 で証明する．

演習 2.17: 正規行列の固有値が実数であるときにのみ，正規行列は Hermite 行列であることを示せ．

$U^\dagger U = I$ ならば行列 U は**ユニタリー** (unitary) であるという．同様にオペレータ U は $U^\dagger U = I$ ならばユニタリーである．オペレータがユニタリーであるのは，その行列表現がユニタリーであるときのみであることが容易に確認できる．ユニタリーオペレータは $UU^\dagger = I$ も満たすので，U は正規でありスペクトル分解ができる．幾何学的にユニタリーオペレータはベクトル間の内積を保存するので重要である．これを見るために $|v\rangle$ と $|w\rangle$ を任意の 2 つのベクトルとすると，$U|v\rangle$ と $U|w\rangle$ の内積は $|v\rangle$ と $|w\rangle$ の内積に等しい．

$$(U|v\rangle, U|w\rangle) = \langle v|U^\dagger U|w\rangle = \langle v|I|w\rangle = \langle v|w\rangle. \tag{2.36}$$

この結果は，任意のユニタリーオペレータ U は次のようなすっきりした外積表現ができることを示している．$|v_i\rangle$ は任意の正規直交基底の集合であるとする．$|w_i\rangle \equiv U|v_i\rangle$ を定義すると，ユニタリーオペレータは内積を保存するので $|w_i\rangle$ も正規直交基底の集合である．$U = \sum_i |w_i\rangle\langle v_i|$ が成り立つ．逆にもし $|v\rangle$ と $|w\rangle$ が任意の 2 つの正規直交基底ならば，$U \equiv \sum_i |w_i\rangle\langle v_i|$ で定義されるオペレータ U はユニタリーオペレータであることが容易に確認できる．

演習 2.18: ユニタリー行列のすべての固有値は絶対値 (modulus) が 1 である，つまり固有値はある実数 θ を用いて $e^{i\theta}$ の形で書けることを示せ．

演習 2.19: **（Pauli の行列：Hermite 性とユニタリー性）** Pauli の行列は Hermite 行列でかつユニタリーであることを示せ．

演習 2.20:（基底の変更） 2 つの異なる正規直交基底 $|v_i\rangle$ と $|w_i\rangle$ に関する，ベクトル空間 V 上のオペレータ A の行列表現が A' と A'' であるとする．このとき，A' と A'' の要素は $A'_{ij} = \langle v_i|A|v_j\rangle$ および $A''_{ij} = \langle w_i|A|w_j\rangle$ である．A' と A'' の関係を求めよ．

Hermite オペレータのうちで，ある特別の部分クラスは非常に重要である．それは **正のオペレータ** (positive operator) である．正のオペレータは任意のベクトル $|v\rangle$ に対して $(|v\rangle, A|v\rangle)$ が実数で負でない数となるオペレータ A として定義される．もし $(|v\rangle, A|v\rangle)$ が $|v\rangle \neq 0$ に対して **厳密に** 0 より大きければ，A は **正の定符号** (positive definite) であるという．演習 2.24 では任意の正のオペレータは自動的に Hermite オペレータとなり，したがってスペクトル分解により負でない固有値 λ_i を用いて対角表現 $\sum_i \lambda_i|i\rangle\langle i|$ ができるのを示すことを課題とする．

演習 2.21: M が Hermite オペレータの場合にコラム 2.2 と同じスペクトル分解の証明を，可能なところは簡略化して行え．

演習 2.22: Hermite オペレータの異なる固有値を持つ 2 つの固有ベクトルは直交することを証明せよ．

演習 2.23: 射影オペレータ P の固有値はすべて 0 か 1 であることを示せ．

演習 2.24:（正のオペレータの Hermite 性） 正のオペレータは必ず Hermite オペレータであることを示せ．（ヒント：任意のオペレータ A は，B と C が Hermite オペレータであるとして，$A = B + iC$ と書けることを示せ.）

演習 2.25: 任意のオペレータ A に対して $A^\dagger A$ が正であることを示せ．

コラム 2.2: スペクトル分解 — 重要！

スペクトル分解 (spectral decomposition) は正規オペレータに対して非常に有用な表現に関する定理である．

定理 2.1:（スペクトル分解） ベクトル空間 V 上の任意の正規オペレータ M は V のある正規直交基底に関して対角である．逆に任意の対角化

可能なオペレータは正規である．

証明　逆方向は簡単な演習なので，順方向のみをベクトル空間 V の次元 d に関する帰納法を使って証明する．$d=1$ の場合は自明である．λ を M の固有値，P を λ の固有空間への射影オペレータ，Q を直交相補空間への射影オペレータとする．このとき $M=(P+Q)M(P+Q)=PMP+QMP+PMQ+QMQ$ である．ここで明らかに $PMP=\lambda P$ である．さらに M は部分空間 P をそれ自身に変換するので $QMP=0$ となる．同様に $PMQ=0$ であることもいえる．それは $|v\rangle$ を部分空間 P の要素とすると $MM^\dagger|v\rangle=M^\dagger M|v\rangle=\lambda M^\dagger|v\rangle$ となる．したがって，$M^\dagger|v\rangle$ は固有値 λ を有し，したがって部分空間 P の要素である．これにより $QM^\dagger P=0$．この式の転置共役をとると $PMQ=0$ となる．以上より $M=PMP+QMQ$ となる．次に QMQ が正規であることを証明する．$QM=QM(P+Q)=QMQ$ および $QM^\dagger=QM^\dagger(P+Q)=QM^\dagger Q$ であることに注意すると，M が正規であるので $Q^2=Q$ も考慮して

$$
\begin{aligned}
QMQQM^\dagger Q &= QMQM^\dagger Q && (2.37)\\
&= QMM^\dagger Q && (2.38)\\
&= QM^\dagger MQ && (2.39)\\
&= QM^\dagger QMQ && (2.40)\\
&= QM^\dagger QQMQ && (2.41)
\end{aligned}
$$

となる．したがって QMQ は正規である．帰納法により QMQ は部分空間 Q のある正規直交基底に関して対角であり，PMP はすでに P のある正規直交基底に関して対角である．この結果 $M=PMP+QMQ$ は全ベクトル空間に対するある正規直交基底に関して対角である．　□

外積表現では，この定理は M が $M=\sum_i \lambda_i|i\rangle\langle i|$ と書けることを意味する．ここで λ_i は M の固有値，$|i\rangle$ は V の正規直交基底，各 $|i\rangle$ は固有値 λ_i に対応する M の固有ベクトルである．射影オペレータで表すと $M=\sum_i \lambda_i P_i$ となる，ただし λ_i は M の固有値，P_i は λ_i の固有空間への射影オペレー

タである．これらの射影オペレータは完全性関係 $\sum_i P_i = I$ と正規直交関係 $P_i P_j = \delta_{ij} P_i$ を満たす．

2.1.7 テンソル積

テンソル積 (tensor product) はベクトル空間を組み合わせて，大きなベクトル空間を形成する方法である．この方法は多粒子系の量子力学を理解するのに重要である．ここでの議論は多少抽象的であるため，テンソル積に慣れていない読者には読みにくいかも知れない．したがって最初はスキップして，後で量子力学でテンソル積の議論が必要になれば読み返すとよい．

V と W はそれぞれ m 次元と n 次元のベクトル空間であるとする．便宜上 V と W は Hilbert 空間とする．このとき $V \otimes W$ （「V テンソル W」と読む）は mn 次元のベクトル空間である．$V \otimes W$ の要素は V の要素 $|v\rangle$ と W の要素 $|w\rangle$ の「テンソル積」 $|v\rangle \otimes |w\rangle$ の線形結合である．特にもし $|i\rangle$ と $|j\rangle$ が空間 V と W の正規直交基底ならば，$|i\rangle \otimes |j\rangle$ は $V \otimes W$ に対する基底になる．テンソル積 $|v\rangle \otimes |w\rangle$ の簡略記号として，$|v\rangle|w\rangle$，$|v, w\rangle$ さらには $|vw\rangle$ をしばしば用いる．例えば V を基底ベクトル $|0\rangle$ と $|1\rangle$ を有する 2 次元ベクトル空間 V とすると $|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle$ が $V \otimes V$ の要素となる．

定義によってテンソル積は次の基本的性質を満たす：

(1) 任意のスカラー z，V の要素 $|v\rangle$，W の要素 $|w\rangle$ に対して

$$z(|v\rangle \otimes |w\rangle) = (z|v\rangle) \otimes |w\rangle = |v\rangle \otimes (z|w\rangle). \tag{2.42}$$

(2) V の任意の要素 $|v_1\rangle$ と $|v_2\rangle$，W の要素 $|w\rangle$ に対して

$$(|v_1\rangle + |v_2\rangle) \otimes |w\rangle = |v_1\rangle \otimes |w\rangle + |v_2\rangle \otimes |w\rangle. \tag{2.43}$$

(3) 任意の V の要素 $|v\rangle$，W の要素 $|w_1\rangle$ と $|w_2\rangle$ に対して

$$|v\rangle \otimes (|w_1\rangle + |w_2\rangle) = |v\rangle \otimes |w_1\rangle + |v\rangle \otimes |w_2\rangle. \tag{2.44}$$

空間 $V \otimes W$ 上で作用する線形オペレータはどのようなものであろうか？ $|v\rangle$ と $|w\rangle$ を V, W 上のベクトル，A と B をそれぞれ V, W 上のオペレータとすると，$V \otimes W$ 上の線形オペレータ $A \otimes B$ は次式で定義される．

$$(A \otimes B)(|v\rangle \otimes |w\rangle) \equiv A|v\rangle \otimes B|w\rangle. \tag{2.45}$$

$A \otimes B$ の定義は $A \otimes B$ の線形性を保って，$V \otimes W$ の全要素に自然に拡張できる．

$$(A \otimes B)\left(\sum_i a_i|v_i\rangle \otimes |w_i\rangle\right) \equiv \sum_i a_i A|v_u\rangle \otimes B|w_i\rangle \tag{2.46}$$

である．このように定義した $A \otimes B$ は $V \otimes W$ 上で明らかに線形オペレータである．2 つのオペレータのテンソル積の意味は，異なるベクトル空間の間の写像 $A: V \to V'$ と $B: W \to W'$ の場合にも拡張できるのは明らかである．実際 $V \otimes W$ から $V' \otimes W'$ に写像する任意の線形オペレータ C は，V から V' および W から W' に写像するオペレータのテンソル積の線形結合

$$C = \sum_i c_i A_i \otimes B_i \tag{2.47}$$

で表現される．ここで定義により

$$\left(\sum_i c_i A_i \otimes B_i\right)|v\rangle \otimes |w\rangle \equiv \sum_i c_i A_i|v\rangle \otimes B_i|w\rangle \tag{2.48}$$

である．

空間 V, W 上での内積を使って $V \otimes W$ 上の内積を自然に定義できる．

$$\left(\sum_i a_i|v_i\rangle \otimes |w_i\rangle, \sum_j b_j|v'_j\rangle \otimes |w'_j\rangle\right) \equiv \sum_{ij} a_i^* b_j \langle v_i|v'_j\rangle\langle w_i|w'_j\rangle. \tag{2.49}$$

このように定義した関数は内積の定義を満たすことが示せる．この内積の定義から内積空間 $V \otimes W$ は，我々がよく知っている転置共役性，ユニタリー性，正規性，Hermite 性などの性質を継承する．

ここまでの議論は少し抽象的であった．**Kronecker 積** (Kronecker product) と呼ぶ便利な行列表現にすると，もっと具体的になる．A は m 行 n 列の行列，

B は p 行 q 列の行列でとする．このとき次の行列表現が得られる．

$$A \otimes B \equiv \overbrace{\left[\begin{array}{cccc} A_{11}B & A_{12}B & \dots & A_{1n}B \\ A_{21}B & A_{22}B & \dots & A_{2n}B \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1}B & A_{m2}B & \dots & A_{mn}B \end{array}\right]}^{nq\ \text{列}} \left.\vphantom{\begin{array}{c} A \\ A \\ \vdots \\ A \end{array}}\right\} mp\ \text{行}. \tag{2.50}$$

この表現において $A_{11}B$ のような項は p 行 q 列の部分行列を示す．この部分行列の各要素は行列 B のそれに比例し，すべての比例定数は A_{11} である．例えばベクトル $(1,2)$ と $(2,3)$ の積はベクトルであり，

$$\left[\begin{array}{c} 1 \\ 2 \end{array}\right] \otimes \left[\begin{array}{c} 2 \\ 3 \end{array}\right] = \left[\begin{array}{c} 1 \times 2 \\ 1 \times 3 \\ 2 \times 2 \\ 2 \times 3 \end{array}\right] = \left[\begin{array}{c} 2 \\ 3 \\ 4 \\ 6 \end{array}\right]. \tag{2.51}$$

Pauli の行列 X，Y のテンソル積は

$$X \otimes Y = \left[\begin{array}{cc} 0 \cdot Y & 1 \cdot Y \\ 1 \cdot Y & 0 \cdot Y \end{array}\right] = \left[\begin{array}{cccc} 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \\ 0 & -i & 0 & 0 \\ i & 0 & 0 & 0 \end{array}\right] \tag{2.52}$$

である．最後に便利な記号である $|\psi\rangle^{\otimes k}$ について述べる．これは $|\psi\rangle$ それ自身のテンソル積を k 回施したものである．例えば $|\psi\rangle^{\otimes 2} = |\psi\rangle \otimes |\psi\rangle$ である．テンソル積空間の演算に対しても同様の記号が用いられる．

演習 2.26: $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ とする．$|\psi\rangle^{\otimes 2}$ と $|\psi\rangle^{\otimes 3}$ を $|0\rangle|1\rangle$ のようなテンソル積の形と Kronecker 積の形で書き下せ．

演習 2.27: Pauli オペレータの次のテンソル積の行列表現を求めよ．(a) X と Z，(b) I と X，(c) X と I．テンソル積は可換か？

演習 2.28: 転置，複素共役，転置共役の分配則がテンソル積に適用できることを示せ．

$$(A \otimes B)^* = A^* \otimes A^*;\ (A \otimes B)^T = A^T \otimes B^T;$$
$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger. \tag{2.53}$$

演習 2.29: 2 つのユニタリーオペレータのテンソル積はユニタリーオペレータであることを示せ.

演習 2.30: 2 つの Hermite オペレータのテンソル積は Hermite オペレータであることを示せ.

演習 2.31: 2 つの正のオペレータのテンソル積は正のオペレータであることを示せ.

演習 2.32: 2 つの射影オペレータのテンソル積は射影オペレータであることを示せ.

演習 2.33: 1 個の q ビットに働く Hadamard オペレータは次のように書ける.

$$H = \frac{1}{\sqrt{2}}[(|0\rangle + |1\rangle)\langle 0| + (|0\rangle - |1\rangle)\langle 1|]. \tag{2.54}$$

n 個の q ビットに対する Hadamard 変換 $H^{\otimes n}$ は次のように書けることを明示的に示せ.

$$H^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x,y} (-1)^{x \cdot y} |x\rangle\langle y|. \tag{2.55}$$

$H^{\otimes 2}$ に対する行列表現を明示的に書け.

2.1.8　オペレータ関数

オペレータと行列に対して定義される関数には重要なものが多い. 一般に複素数から複素数への関数 f が与えられると, 次のような方法で正規行列（または Hermite 行列のような部分クラス）に対応する行列の関数を定義する. 正規オペレータ A のスペクトル分解を $A = \sum_a a|a\rangle\langle a|$ とする. $f(A) \equiv \sum_a f(a)|a\rangle\langle a|$ を定義する. 少し考えると $f(A)$ は一意に定まることが示せる. この手法は, 例えば正のオペレータの平方根, 正の定符号オペレータの対数, あるいは正規オペ

レータのベキ指数を定義するのに使える．一例をあげると，Z は固有ベクトル $|0\rangle$, $|1\rangle$ を持つので，

$$\exp(\theta Z) = \begin{bmatrix} e^{\theta} & 0 \\ 0 & e^{-\theta} \end{bmatrix} \tag{2.56}$$

となる．

演習 2.34: 次の行列の平方根と対数を求めよ．

$$\begin{bmatrix} 4 & 3 \\ 3 & 4 \end{bmatrix}. \tag{2.57}$$

演習 2.35:（Pauli 行列の指数関数） $\vec{v}$ を任意の 3 次元実数単位ベクトル，θ を実数とする．次式を証明せよ．

$$\exp(i\theta\vec{v}\cdot\vec{\sigma}) = \cos(\theta)I + i\sin(\theta)\vec{v}\cdot\vec{\sigma}, \tag{2.58}$$

ここで $\vec{v}\cdot\vec{\sigma} \equiv \sum_{i=1}^{3} v_i\sigma_i$ である．この演習は問題 2.1 で一般化される．

もう 1 つの重要な行列の関数は行列の**トレース** (trace) である．A のトレースは対角要素の和として定義される．

$$\mathrm{tr}(A) \equiv \sum_i A_{ii}. \tag{2.59}$$

トレースは**巡回不変性** (cyclic)：$\mathrm{tr}(AB) = \mathrm{tr}(BA)$，**線形性** (linear)：$\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B)$，$\mathrm{tr}(zA) = z\mathrm{tr}(A)$ という性質を持つ．ここで A と B は任意の行列，z は複素数である．さらに巡回不変性から，ユニタリーな**相似変換** (similarity transform) $A \to UAU^\dagger$ に対して行列のトレースは不変であることがいえる．すなわち $\mathrm{tr}(UAU^\dagger) = \mathrm{tr}(U^\dagger UA) = \mathrm{tr}(A)$ である．この結果を考えるとオペレータ A のトレースを A の行列表現のトレースであると定義するのが道理にかなう．この場合ユニタリーな相似変換でトレースが不変になるので，オペレータのトレースが明確に定義されている．

トレースの例をあげる．$|\psi\rangle$ は単位ベクトル，A は任意のオペレータとして $\mathrm{tr}(A|\psi\rangle\langle\psi|)$ を計算するために，Gram-Schmidt 手順を使って $|\psi\rangle$ を第 1 要素として含む正規直交基底 $|i\rangle$ で展開する．そうすると

$$\mathrm{tr}(A|\psi\rangle\langle\psi|) = \sum_i \langle i|A|\psi\rangle\langle\psi|i\rangle \tag{2.60}$$

$$= \langle\psi|A|\psi\rangle \tag{2.61}$$

が得られる．この $\mathrm{tr}(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle$ という結果はオペレータのトレースを求めるときに非常に便利である．

演習 2.36: Paili の行列のトレースは I 以外はゼロであることを示せ．

演習 2.37:（トレースの巡回不変性） A と B が 2 つの線形オペレータならば

$$\mathrm{tr}(AB) = \mathrm{tr}(BA) \tag{2.62}$$

であることを示せ．

演習 2.38:（トレースの線形性） A と B が線形オペレータならば

$$\mathrm{tr}(A+B) = \mathrm{tr}(A) + \mathrm{tr}(B) \tag{2.63}$$

であることを示せ．また z が任意の複素数ならば

$$\mathrm{tr}(zA) = z\mathrm{tr}(A) \tag{2.64}$$

であることを示せ．

演習 2.39:（オペレータに対する Hilbert-Schmidt の内積） Hilbert 空間 V の線形オペレータ集合 L_V は明らかにベクトル空間を形成する．つまり 2 つの線形オペレータの和は線形オペレータ，A が線形オペレータで z が複素数ならば zA は線形オペレータ，そしてゼロ要素 0 が存在する．もう 1 つの重要な結果はベクトル空間 L_V には自然に内積構造を導入することができるので，Hilbert 空間となり得ることである．

(1) $L_V \times L_V$ 上で

$$(A, B) \equiv \mathrm{tr}(A^\dagger B) \tag{2.65}$$

により定義される関数 $(\cdot, \cdot)$ は内積関数であることを示せ．この内積を **Hilbert-Schmidt の内積** (Hilbert-Schmidt inner product) または **トレース内積** (trace inner product) と呼ぶ．

(2) もし V が d 次元ならば，L_V は d^2 次元であることを示せ．

(3) Hilbert 空間 L_V に対する Hermite 行列の正規直交基底を求めよ．

2.1.9 交換子と反交換子

2 つのオペレータ A, B の**交換子** (commutator) は次式で定義される．

$$[A, B] \equiv AB - BA. \tag{2.66}$$

もし $[A, B] = 0$ つまり $AB = BA$ ならば A は B と**可換** (commute) であるという．同様に 2 つのオペレータ A, B の **反交換子** (anti-commutator) は次式で定義される．

$$\{A, B\} \equiv AB + BA. \tag{2.67}$$

もし $\{A, B\} = 0$ ならば，A は B と **反可換** (anti-commute) であるという．交換子と反交換子から 2 つのオペレータの多くの重要な性質が導かれる．多分最も有用な関係式は，交換子と **同時対角化** (simultaneouly diagonalize) できる Hermite オペレータ A, B の間の関係である．同時対角化できるとは A, B の固有ベクトルに共通の正規直交集合 $|i\rangle$ を用いて $A = \sum_i a_i |i\rangle\langle i|$，$B = \sum_i b_i |i\rangle\langle i|$ と書けることである．

定理 2.2:（同時対角化定理） A と B が Hermite オペレータであるとする．A と B を同時に対角化できる正規直交基底が存在するとき，そのときにのみ $[A, B] = 0$ となる．この場合に A と B は **同時対角化可能** (simultaneously diangnalizable) であるという．

この結果は，計算するのが簡単な2つのオペレータの交換子と，前もって決めるのが難しい同時対角化の可能性を関係付けるものである．例えば次の式を考える．

$$[X,Y] = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} - \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \tag{2.68}$$

$$= 2i\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{2.69}$$

$$= 2iZ, \tag{2.70}$$

よって X と Y は可換でない．演習 2.11 で X と Y は共通の固有ベクトルを持たないことを示したが，同じく同時対角化定理からも予想できる．

証明　A と B が同じ正規直交基底において対角ならば，$[A,B]=0$ であることは容易に証明できる（し，証明すべきである！）．逆を示すのに，まず $|a,j\rangle$ を固有値 a を持つ A の固有空間 V_a に対する正規直交基底であるとする．j は縮退の可能性に備える指数である．

$$AB|a,j\rangle = BA|a,j\rangle = aB|a,j\rangle \tag{2.71}$$

なので $B|a,j\rangle$ は固有空間 V_a の要素である．P_a が空間 V_a への射影オペレータであるとして，$B_a \equiv P_aBP_a$ を定義する．B_a を空間 V_a に限定すると V_a 上の Hermite オペレータとなり，したがって空間 V_a を張る固有ベクトルの正規直交集合でスペクトル分解できることが容易にわかる．この固有ベクトルを $|a,b,k\rangle$ と書く．ここで指数 a, b は A, B_a の固有値のラベル，k は B_a の縮退の可能性を考慮した指数である．$B|a,b,k\rangle$ は V_a の要素なので $B|a,b,k\rangle = P_aB|a,b,k\rangle$ である．さらに $P_a|a,b,k\rangle = |a,b,k\rangle$ なので

$$B|a,b,k\rangle = P_aBP_a|a,b,k\rangle = b|a,b,k\rangle. \tag{2.72}$$

この結果 $|a,b,k\rangle$ は B の固有ベクトルで固有値 b を持つ．したがって $|a,b,k\rangle$ は A と B の両方の固有ベクトルの正規直交集合であり，A と B が定義されている全ベクトル空間の基底を張る．つまり A と B は同時に対角化可能である．□

演習 2.40:（Pauli の行列の交換関係） 次の交換関係を証明せよ．

$$[X,Y]=2iZ;\quad [Y,Z]=2iX;\quad [Z,X]=2iY. \tag{2.73}$$

3 つの指数 $\{j,k,l\}$ の反対称テンソル ϵ_{jkl} を用いて，この式を表すスマートな方法がある．

$$[\sigma_j,\sigma_k]=2i\sum_{l=1}^{3}\epsilon_{jkl}\sigma_l, \tag{2.74}$$

ここで $\epsilon_{123}=\epsilon_{231}=\epsilon_{312}=1$，$\epsilon_{321}=\epsilon_{213}=\epsilon_{132}=-1$，それ以外は $\epsilon_{jkl}=0$ である．

演習 2.41:（Pauli の行列の反交換関係） $i\neq j$ なる i, j が両方とも集合 $\{1,2,3\}$ から選ばれるとき，

$$\{\sigma_i,\sigma_j\}=0 \tag{2.75}$$

であることを証明せよ．また $i=0,1,2,3$ に対して次式を証明せよ．

$$\sigma_i^2=I. \tag{2.76}$$

演習 2.42: 次の式を示せ．

$$AB=\frac{[A,B]+\{A,B\}}{2}. \tag{2.77}$$

演習 2.43: $j,k=1,2,3$ に対して次式を示せ．

$$\sigma_j\sigma_k=\delta_{jk}I+i\sum_{l=1}^{3}\epsilon_{jkl}\sigma_l. \tag{2.78}$$

演習 2.44: $[A,B]=0$，$\{A,B\}=0$ および A は可逆であるならば，B は 0 でなければならないことを示せ．

演習 2.45: $[A,B]^\dagger=[B^\dagger,A^\dagger]$ であることを示せ．

演習 2.46: $[A,B]=-[B,A]$ であることを示せ．

演習 2.47: A と B は Hermite オペレータであるならば，$i[A,B]$ は Hermite オペレータであることを示せ．

2.1.10 極分解と特異値分解

極分解 (polar decomposition) と**特異値分解**(singular value decomposition) は線形オペレータをより簡単な部分に分割する便利な方法である．特にこれらの分解により一般の線形オペレータをユニタリーオペレータと正オペレータの積に分けることができる．一般の線形オペレータに対する構造についてはほとんど学習していないが，ユニタリーオペレータと正のオペレータについてはかなり理解が進んでいる．極分解と特異値分解によってこの理解を一般の線形オペレータの理解へ広げることができる．

定理 2.3: **（極分解）** A をベクトル空間 V 上の線形オペレータとする．次式を満たすユニタリーオペレータ U と正のオペレータ J, K が存在する．

$$A = UJ = KU. \tag{2.79}$$

この式を満たす一意の正のオペレータ J, K は $J \equiv \sqrt{A^\dagger A}$, $K \equiv \sqrt{AA^\dagger}$ で定義される．さらにもし A が可逆 (invertible) ならば U は一意に決まる．

式 $A = UJ$ を A の**左極分解** (left polar decomposition)，$A = KU$ を A の**右極分解** (right polar decomposition) と呼ぶ．しばしば「右」「左」の言葉を省略して両方を「極分解」と呼び，文脈で判断することが多い．

証明 $J \equiv \sqrt{A^\dagger A}$ は正のオペレータであり，スペクトル分解 $J = \sum_i \lambda_i |i\rangle\langle i|$, $(\lambda_i \geq 0)$ ができる．$|\psi_i\rangle \equiv A|i\rangle$ を定義する．この定義より $\langle\psi_i|\psi_i\rangle = \lambda_i^2$ がわかる．当面 $\lambda_i \neq 0$ である i だけを考える．この i に対して $|e_i\rangle \equiv |\psi_i\rangle/\lambda_i$ を定義すると，$|e_i\rangle$ は正規化される．さらにもし $i \neq j$ ならば $\langle e_i|e_j\rangle = \langle i|A^\dagger A|j\rangle/\lambda_i\lambda_j = \langle i|J^2|j\rangle/\lambda_i\lambda_j = 0$ なので，$|e_i\rangle$ は直交している．

我々は $\lambda_i \neq 0$ なる i を考えてきた．次に Gram-Schmidt の手続きを用いて，正規直交集合 $|e_i\rangle$ を拡張して正規直交基底とし，これにも $|e_i\rangle$ のラベルを付ける．ユニタリーオペレータ $U \equiv \sum_i |e_i\rangle\langle i|$ を定義する．$\lambda_i \neq 0$ のとき $UJ|i\rangle = \lambda_i|e_i\rangle = |\psi_i\rangle = A|i\rangle$ が成り立つ．$\lambda_i = 0$ のときには $UJ|i\rangle = 0 = |\psi_i\rangle$ である．基底 $|i\rangle$ 上で A と UJ の作用が一致すること，つまり $A = UJ$ であることが証明された．

$A = UJ$ に左から転置共役式 $A^\dagger = JU^\dagger$ を掛けると，$J^2 = A^\dagger A$ となり $J = \sqrt{A^\dagger A}$ が一意に得られるので J は一意である．少し考えると A が可逆ならば J も可逆であり，U は式 $U = AJ^{-1}$ により一意に決まる．右極分解の証明は次の通りである．$K \equiv UJU^\dagger$ が正のオペレータであるとすると $A = UJ = UJU^\dagger U = KU$ である．$AA^\dagger = KUU^\dagger K = K^2$ なので $K = \sqrt{AA^\dagger}$ でなければならず，よって定理は証明された． □

特異値分解は極分解とスペクトル分解定理を組み合わせたものである．

系 2.4:（特異値分解） A を正方行列とする．このとき

$$A = UDV \tag{2.80}$$

を満たすユニタリー行列 U, V と負でない要素をもつ対角行列 D が存在する．D の対角要素を A の**特異値** (singular valur) と呼ぶ．

証明 極分解によってユニタリー S，正の J に対して $A = SJ$ である．スペクトル定理によって，ユニタリー T，負でない要素を持つ対角 D に対して $J = TDT^\dagger$ である．$U \equiv ST$，$V \equiv T^\dagger$ とおくと証明が完了する． □

演習 2.48: 正の行列 P の極分解は何か？ ユニタリー行列 U，Hermite 行列 H に対してはどうか？

演習 2.49: 外積表現で正規行列の極分解を示せ．

演習 2.50: 次の行列の左および右極分解を求めよ．

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}. \tag{2.81}$$

2.2 量子力学の公理

すべての理解は見かけの世界を受け入れないところから始まる．
— Alan Kay

世界について最も理解できないことは包容力が大きいことである．
— Albert Einstein

量子力学は物理学理論を展開するための数学的枠組みである．量子力学それ自体では物理システムがどのような法則に従うべきかを教えてくれないが，そのような法則を展開するための数学上および概念上の枠組みを提供する．次の数節で量子力学の基本公理の全貌を述べる．これらの公理は量子力学の数学的形式と物理世界との橋渡しをするものである．

量子力学の公理は試行と（その多くは）錯誤の長い過程を経て導かれたものであり，創始者達によるかなりの手探りと推測に満ちている．公理に対する動機が常に明確でなくても驚かないで欲しい．専門家にとっても量子力学の基本公理は驚くべきものなのである．次の数節で読者が得られるものは公理の生きた理解 — 何時どのように適用するか — である．

2.2.1　状態空間

量子力学の最初の公理によって量子力学の活動の舞台が設定される．その舞台は線形代数で身近になった Hilbert 空間である．

公理 1: 任意の孤立した物理システムに関して，システムの**状態空間**(state space) と呼ぶ内積を伴う複素ベクトル空間（つまり Hilbert 空間）が存在する．システムは状態空間の単位ベクトルである**状態ベクトル** (state vector) によって完全に記述できる．

与えられた物理システムに対して，そのシステムの状態空間が何であるかとか，状態ベクトルが何であるかを量子力学は教えてくれない．**特定**のシステムに対してこれらを解決するのは困難な問題であり，このために物理学者は複雑で美しいルールを展開してきた．例えば量子電気力学（quantum electrodynamics，略して QED ）の素晴らしい理論が原子と光の相互作用を記述する．QED の一側面は原子と光を量子力学的に記述するのに用いる状態空間を教えてくれる．多くの場合我々は量子力学が準備する一般的枠組みに関心があるので，（物理的実体に適用する 7 章を除いては）QED のような難解な理論には立ち入らない．我々の目

的には興味を持つシステムの状態空間に関する，簡単な（しかし合理的な）仮定を設けるだけで十分である．

最も簡単で我々が最も関心を持つ量子力学システムは **q ビット** (qubit) である．q ビットは 2 次元状態空間を持つ．$|0\rangle$ と $|1\rangle$ がその状態空間の基底を形成する．そのとき状態空間における任意の状態ベクトルは次のように書ける．

$$|\psi\rangle = a|0\rangle + b|1\rangle, \tag{2.82}$$

ここで a と b は複素数である．$|\psi\rangle$ が単位ベクトルであるという条件 $\langle\psi|\psi\rangle = 1$ は $|a|^2 + |b|^2 = 1$ と等価であり，条件 $\langle\psi|\psi\rangle = 1$ を状態ベクトルの **正規化条件** (normalization condition) と呼ぶ．

我々は q ビットを基本的な量子力学システムと考える．7 章 (第 II 巻) で q ビットが記述できる現実の物理システムが存在することを示す．しかし当面は q ビットを抽象的言葉と捉え特定の事実と対照しなくてもよい．q ビットについて議論するとき，正規直交の基底ベクトル集合 $|0\rangle$ と $|1\rangle$ を常に参照し，その基底は前もって固定していると考える．直観的には状態 $|0\rangle$ と $|1\rangle$ はビットがとる 2 つの値 0 と 1 に相似している．q ビットがビットと異なるのはこれら 2 つの状態の**重ね合せ** (superpsition) $a|0\rangle + b|1\rangle$ が存在し得ることであり，その場合は q ビットが確定的に $|0\rangle$ 状態にあるとか確定的に $|1\rangle$ 状態にあるといえない．

最後に量子状態を記述する際にしばしば使用される便利な言葉を紹介する．任意の線形結合 $\sum_i \alpha_i|\psi_i\rangle$ は状態 $|\psi_i\rangle$ に対する **振幅** (amplitude) α_i を以て状態 $|\psi_i\rangle$ を重ね合せたものである．したがって，例えば

$$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \tag{2.83}$$

は状態 $|0\rangle$ に対して振幅 $1/\sqrt{2}$，状態 $|1\rangle$ に対して振幅 $-1/\sqrt{2}$ で，状態 $|0\rangle$ と $|1\rangle$ を重ね合わせたものである．

2.2.2 時間発展

量子力学システムの状態 $|\psi\rangle$ は時間と共に如何に変化するか？ その状態変化を記述する処方箋が次の公理で与えられる．

公理 2: 閉じた量子システムの時間発展は ユニタリー変換 (unitary transform) で記述される．つまり時刻 t_1 におけるシステムの状態 $|\psi\rangle$ は，時刻 t_2 におけるシステムの状態 $|\psi'\rangle$ と時刻 t_1 と t_2 だけに依存するユニタリーオペレータ U によって関係付けられる．

$$|\psi'\rangle = U|\psi\rangle. \tag{2.84}$$

量子力学が**特定**の量子システムの状態空間や量子状態を教えてくれないのと同様に，実世界の量子ダイナミックスを記述するユニタリーオペレータ U がどのようなものかも教えてくれない．量子力学は閉じた量子システムの時間発展がこのような方法で記述できることを保証するだけである．すぐに湧く疑問はどのようなユニタリーオペレータを考えるのが自然か？ということである．単一 q ビットについては**如何なる**ユニタリーオペレータでも現実世界で実現できることがわかる．

量子計算と量子情報において重要な，単一 q ビットに関するユニタリーオペレータの例を二三見てみよう．すでに我々はそのようなユニタリーオペレータの例を幾つか知っている．2.2.3 項で Pauli の行列を定義したし，1 章では量子ゲートについて述べた．1.3.1 項で述べたように，古典 NOT ゲートのアナロジーから X 行列は量子 NOT ゲートであることが知られている．Pauli の X と Z 行列は**ビット反転** (bit flip) および**位相反転** (phase flip) 行列とも呼ばれる．X 行列は $|0\rangle$ を $|1\rangle$ に $|1\rangle$ を $|0\rangle$ に変換するのでビット反転の名があり，Z 行列は $|0\rangle$ を不変に保つ一方で $|1\rangle$ を $-|1\rangle$ に変換し，付加因子 -1 が**位相因子** (phase factor) なので位相反転の名がある．しかし 4 章 (第 II 巻) で定義する位相ゲートと紛らわしいので Z に対して位相反転という言葉を使うことはあまりない．(2.2.7 項には「位相」という言葉の用例が多く議論されている．)

もう 1 つの興味あるユニタリーオペレータは **Hadamard ゲート** (Hadamard gate) であり H と表記する．このオペレータの作用は $H|0\rangle \equiv (|0\rangle + |1\rangle)/\sqrt{2}$，$H|1\rangle \equiv (|0\rangle - |1\rangle)/\sqrt{2}$ で定義され，行列表現では次のように与えられる：

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{2.85}$$

演習 2.51: Hadamard ゲートがユニタリーであることを証明せよ．

演習 2.52: $H^2 = I$ を証明せよ．

演習 2.53: H の固有値と固有ベクトルは何か？

公理 2 は記述するシステムが閉じていることを要求している．つまり他のシステムと相互作用をしていない．もちろん実際には（全宇宙を除いて）すべてのシステムは少なくとも多少は他のシステムと相互作用する．にもかかわらず閉じているという近似がよく成り立ち，ユニタリー時間発展で記述できる興味深いシステムがある．さらに，少なくとも原理上すべての開かれたシステムはユニタリー時間発展をするより大きな閉じたシステム（宇宙）の一部として記述できる．後で閉じていないシステムを記述するツールを紹介するが，さし当たり閉じたシステムの時間発展に関する記述を進める．

公理 2 は 2 つの異なる時刻における閉じた量子状態がどのように関係するかについて述べている．この公理を発展させると，量子システムの進化を**連続時間** (continuous time) で記述できる．この発展した公理から公理 2 を回復することもできる．改訂版の公理を述べる前に 2 つのことを述べておく．第 1 は表記法上の注意である．次の議論に現れる H は少し前に紹介した Hadamard オペレータと同じではない．第 2 に次の公理には微分方程式が使われる．微分方程式に親しみのない読者も（量子情報処理の物理的実現に関する 7 章 (第 II 巻) の一部を除いて）本書の大部分では微分の知識を必要としないので安心してよい．

公理 2′: 閉じた量子システムの状態の時間発展は **Schrödinger 方程式** (Schrödinger equation)

$$i\hbar \frac{d|\psi\rangle}{dt} = H|\psi\rangle \tag{2.86}$$

で記述される．ここで $\hbar$ は **Planck の定数**(Planck's constant) であり，その値は実験で決められる．その正確な値は我々には重要でない．実際 $\hbar$ を H に吸収させ実効的に $\hbar = 1$ と置くことが多い．H は Hermite オペレータであり，閉じたシステムの**ハミルトニアン** (Hamiltonian) と呼ぶ．

システムの Hamiltonian がわかれば（$\hbar$ もわかっているとして），少なくとも原理上はダイナミックスを完全に理解できる．実際に特定の物理システムを記述するに必要な Hamiltonian を求めることは非常に難しい問題であって，これに答

えるには相当量の実験による情報入力が要求され，20 世紀物理学の多くはこの問題に関わってきた．我々の立場では，この問題は量子力学それ自身の理論で取り扱う問題ではなく，量子力学の枠組みの中で構築される個別の物理学理論が取り扱うべき — これこれの構造を持つ原子を記述する Hamiltonian は何かというような — **詳細** な問題である．量子計算と量子情報に関する我々の議論の多くでは Hamiltonian それ自身を議論する必要はなく，議論の出発点としてある行列が Hamiltonian であると仮定して，その Hamiltonian を使うのが妥当かどうかについては敢えて議論せずに先に進む．

Hamiltonian は Hermite オペレータなので，固有値 E とそれに対応する正規化固有ベクトル $|E\rangle$ を用いてスペクトル分解できる．

$$H = \sum_E E|E\rangle\langle E|. \tag{2.87}$$

状態 $|E\rangle$ は通常**エネルギー固有状態**(energy eigenstate) または**定常状態** (stationary state) とも呼ばれ，E は状態 $|E\rangle$ の**エネルギー** (energy) である．最も低いエネルギーはシステムの**基底状態エネルギー** (ground state energy) といい，対応するエネルギー固有状態（または固有空間）を **基底状態** (ground state) という．$|E\rangle$ を定常状態と呼ぶのは，唯一の時間変化が全体に掛かる位相因子にのみ現れるのが理由である．

$$|E\rangle \rightarrow \exp(-iEt/\hbar)|E\rangle. \tag{2.88}$$

例えば単一 q ビットの Hamiltonian が Pauli の行列のみを用いて

$$H = \hbar\omega X \tag{2.89}$$

で与えられるとする．この式で ω は実験で決めるべきパラメータである．このパラメータについてここでは気にしないことにする．要は量子計算と量子情報の研究で登場する Hamiltonian を読者に感じてもらえればそれでよい．この Hamiltonian のエネルギー固有状態は明らかに X の固有状態と同じであり，状態が $(|0\rangle+|1\rangle)/\sqrt{2}$ と $(|0\rangle-|1\rangle)/\sqrt{2}$，それぞれに対応するエネルギーが $\hbar\omega$ と $-\hbar\omega$ で与えられる．したがって基底状態は $(|0\rangle-|1\rangle)/\sqrt{2}$，基底状態エネルギーは $-\hbar\omega$ である．

ダイナミックスを記述する Hamiltonian 描像の公理 2′ とユニタリーオペレータ描像の公理 2 はどのような関係にあるか？ その答えは Schrödinger 方程式の解

を書き下すと得られ，次式がが容易に証明できる：

$$|\psi(t_2)\rangle = \exp\left[\frac{-iH(t_2 - t_1)}{\hbar}\right]|\psi(t_1)\rangle = U(t_1, t_2)|\psi(t_1)\rangle, \tag{2.90}$$

ここで

$$U(t_1, t_2) \equiv \exp\left[\frac{-iH(t_1 - t_2)}{\hbar}\right] \tag{2.91}$$

と定義する．演習においてこのオペレータはユニタリーであり，さらに任意のユニタリーオペレータ U はある Hermite オペレータ K に対して $U = \exp iK$ の形で実現できることを示す．したがって，ユニタリーオペレータを用いた離散時間におけるダイナミックスの記述と，Hamiltonian を用いた連続時間の記述には 1：1 の対応がある．本書の大部分では量子ダイナミックスのユニタリー形式を用いる．

演習 2.54: A と B は可換な Hermite オペレータであるとする．$\exp(A)\exp(B) = \exp(A + B)$ を証明せよ．（ヒント：2.1.9 項の結果を使え．）

演習 2.55: 式 (2.91) で定義された $U(t_1, t_2)$ がユニタリーであることを示せ．

演習 2.56: スペクトル分解を用いて，任意のユニタリーオペレータ U に対して $K \equiv -i\log(U)$ が Hermite オペレータであり，したがってある Hermite オペレータ K に対して $U = \exp(iK)$ となることを示せ．

量子計算と量子情報において特定の量子システムにユニタリーオペレータを適用 (apply) するという表現をよくする．例えば量子回路の文脈で単一 q ビットにユニタリーゲートを適用するという．これは前にユニタリーオペレータが閉じた量子システムの進化を記述すると述べたことと矛盾しないか？ 結局我々がユニタリーオペレータを適用するということは，量子システムと相互作用する「我々」が外部にいてシステムは閉じられていないのである．

この例はレーザ光を原子に集束したときに起きる．多くの思索と苦しい仕事の末に全原子・レーザシステムを記述する Hamiltonian を書き下すことができている．興味深いことに原子・レーザシステムの Hamiltonian を書き下した後で原子だけへの効果を考えると，全く完全にではないがほとんど完全に，原子の状態ベ

クトルは別の Hamiltonian である**原子の Hamiltonian** (atomic Hamiltonian) で記述できる．原子の Hamiltonian にはレーザ強度や他のレーザパラメータに関する項があり，それを意のままに変化させることができる．それは**あたかも**原子が閉じたシステムではなく，我々の意のままに変えられる Hamiltonian によって原子の時間発展記述されるのと同じである．

一般にこのような多くのシステムに対して，システム Hamiltonian が一定でなく実験家の意のままになるパラメータによって変化し，実験の途中で変化するような，量子システムの**時間変化**をする Hamiltonian を書き下すことができる．したがって，システムは閉じていないが，時間変化をする Hamiltonian を有する Schrödinder 方程式に従って良い近似で時間発展する．

結論として我々は最初は量子システムの時間発展を — 閉じたシステムでなくても — しばしばユニタリーオペレータを用いて記述する．重要な例外は量子測定でありこれについては次の項で述べる．もう少し進むと，他のシステムとの相互作用により生じるユニタリー時間発展からのずれの可能性を詳しく調べて，現実の量子システムのダイナミックスをより正確に理解することができる．

2.2.3　量子測定

閉じた量子システムはユニタリー時間発展に則って変化すると仮定した．残り他の世界と相互作用のないシステムの時間発展はそれでよい．しかし実験家と実験装置 — つまり外部の物理システム — がシステムを観測して，システム内部で何が起きているかを見ようとするときもなければならない．この相互作用においてシステムはもはや閉じてはおらず，したがってユニタリー時間発展にならない．これがなされたときに何が起きるかを説明するために，公理 3 を導入して量子システムに対する測定の効果を記述する手法を提供する．

公理 3: 量子測定は**測定オペレータ** (measurement operator) の集まり $\{M_n\}$ で記される．これらオペレータは被測定システムの状態空間に作用する．指数 m は実験で生じる測定結果を指す．もし測定直前の量子システム状態が $|\psi\rangle$ ならば，測定結果 m が生じる確率は

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{2.92}$$

で与えられ，測定後のシステム状態は

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \tag{2.93}$$

である．測定オペレータは次の**完全性の式**を満たす．

$$\sum_m M_m^\dagger M_m = I. \tag{2.94}$$

完全性の式は確率の和が 1 になるという事実を表現する：

$$1 = \sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{2.95}$$

すべての $|\psi\rangle$ に対して満たされるこの式は完全性の式と等価である．しかし，完全性の式のほうが直接容易に証明できるので公理の中に入れた．

簡単であるが重要な測定の例が**計算基底における q ビットの測定**である．これは単一 q ビットに対して，$M_0 = |0\rangle\langle 0|$，$M_1 = |1\rangle\langle 1|$ の 2 つの測定オペレータにより定義され，2 つの結果を出す測定である．各測定オペレータは Hermite オペレータであり $M_0^2 = M_0$，$M_1^2 = M_1$ であることがわかる．したがって，完全性の関係が満たされる：$I = M_0^\dagger M_0 + M_1^\dagger M_1 = M_0 + M_1$．被測定状態は $|\psi\rangle = a|0\rangle + b|1\rangle$ である．このとき測定結果 0 を得る確率は

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = |a|^2. \tag{2.96}$$

同様に測定結果 1 を得る確率は $p(1) = |b|^2$ である．したがって，2 つの場合の測定後の状態は

$$\frac{M_0|\psi\rangle}{|a|} = \frac{a}{|a|}|0\rangle \tag{2.97}$$

$$\frac{M_1|\psi\rangle}{|b|} = \frac{b}{|b|}|1\rangle. \tag{2.98}$$

2.2.7 項で説明するが，$a/|a|$ のような絶対値が 1 の係数は無視してもよく，1 章で述べたように測定後の状態は実効的に $|0\rangle$, $|1\rangle$ となる．

基本公理としての公理 3 は多くの人の興味をかき立てるものである．測定デバイスは量子力学的システムなので，被測定量子システムと測定デバイスはより大

きな孤立した量子力学的システムの一部になる．(完全に孤立したシステムにするには，被測定システムと測定デバイス以外の量子システムを含める必要があるかも知れないが，要点はこれができることにある.）公理 2 によればこの大きな孤立システムの時間発展はユニタリー時間変化で記述できる．この描像の結果として公理 3 を導くことができるか．この方向に沿ってかなり多くの研究がなされたが，これが可能かどうか物理学者の間でまだ一致していない．しかし我々は実利的なアプローチを採用して，実際上場合によって公理 2 と公理 3 を使い分けることとし，一方の公理から他方を導くことに悩まないことにする．

次の数項では幾つかの基本的で重要な測定シナリオに対して公理 3 を適用する．2.2.4 項では量子状態の集合を**識別** (distinguish) する問題を調べる．2.2.5 項では公理 3 の特別な場合である**射影測定** (projective measurement) もしくは **von Neumann の測定** (von Neumann measurement) について説明する．2.2.6 項では公理 3 のもう 1 つ別の特別な場合である，**POVM 測定** (POVM measurement) を説明する．多くの量子力学の入門書では射影測定のみを説明し，公理 3 や POVM 要素の十分な説明を省略している．そこでコラム 2.5 で我々が述べるいろいろなクラスの測定の関係についてコメントする．

演習 2.57:（縦続測定は単一測定） $\{L_l\}$ と $\{M_m\}$ は測定オペレータの 2 つの集合であるとする．測定オペレータ $\{L_l\}$ で定義された測定の後に測定オペレータ $\{M_m\}$ で定義された測定を行うことは，測定オペレータ $\{N_{lm}\}$ で定義された単一の測定を行うことと物理的に等価であることを示せ．ただし $N_{lm} = M_m L_l$ である．

2.2.4　量子状態の識別

公理 3 の重要な応用は**量子状態の識別** (distinguishing quantum state) 問題である．古典的世界では対象物の異なる状態は少なくとも原理上識別可能である．例えばコインを投げたときに，少なくとも理想的極限では表か裏かを識別できる．量子力学では状況が込み入っている．1.6 節では非直交量子状態を識別できないことをもっともらしく議論した．我々は公理 3 を確固たる基礎としてこの事実に納得できる証明を与える．

量子計算と量子情報の多くの概念と同様に，識別可能性を容易に理解するには2人の当事者 Alice と Bob 間のゲームの比喩を用いるのがよい．Alice は両者が知っている固定した状態の集合から1つの状態 $|\psi_i\rangle$ $(1 \le i \le n)$ を選ぶ．彼女はこの状態 $|\psi_i\rangle$ を Bob に与え，彼は Alice から貰った状態の指数 i 言い当てることが求められる．

状態 $|\psi_i\rangle$ は正規直交系であるとする．Bob はこれらの状態を**識別**するために，次の手続きで量子測定を行う．可能な各指数 i に対応して測定オペレータ $M_i \equiv |\psi_i\rangle\langle\psi_i|$ を定義し，もう1つの測定オペレータ M_0 を正のオペレータ $I - \sum_{i\neq 0} |\psi_i\rangle\langle\psi_i|$ の正の平方根として定義する．これらのオペレータは完全性関係を満たす．もし状態 $|\psi_i\rangle$ が準備されると $p(i) = \langle\psi_i|M_i|\psi_i\rangle = 1$，したがって結果 i は確実におきる．したがって，正規直交状態 $|\psi_i\rangle$ を信頼度良く識別することが可能である．

これに対してもしも $|\psi_i\rangle$ が正規直交でなければ，**状態を識別できる量子測定はない**ことが証明できる．この考えでは Bob は測定オペレータ M_j で記述される測定を行い結果 j を得る．この測定結果を用いて Bob は何かあるルール $i = f(j)$ を用いて指数 i を推定しようとする．ここで $f(\cdot)$ は推定するために彼が用いるルールを表す．なぜ Bob が非直交状態 $|\psi_1\rangle$, $|\psi_2\rangle$ を識別できないかという鍵は，$|\psi_2\rangle$ が $|\psi_1\rangle$ に平行な（0 でない）成分と直交する成分に分解できることにある．j が測定結果で $f(j) = 1$，つまり Bob が j を観測して状態 $|\psi_1\rangle$ を推定するとする．しかし $|\psi_2\rangle$ が $|\psi_1\rangle$ に平行な成分を持つために，$|\psi_2\rangle$ が用意されても結果が同じ j となる確率が 0 でない．したがって，Bob は準備された状態をときどき当てそこなう．非直交状態は識別できないというもっと厳密な議論をコラム 2.3 に示すが，ここで述べたのが本質的ポイントである．

コラム 2.3: 非直交状態を完全に識別できない証明

背理法により非直交状態 $|\psi_1\rangle$ と $|\psi_2\rangle$ の識別ができる測定が不可能であることを示す．そのような測定が可能であると仮定する．状態 $|\psi_1\rangle$ (または $|\psi_2\rangle$) を用意すると j を測定して $f(j) = 1$ (または $f(j) = 2$) となる確率は 1 でなければならない．$E_i \equiv \sum_{j:f(j)=i} M_j^\dagger M_j$ を定義するとこれらの観

測は次のように書ける：

$$\langle\psi_1|E_1|\psi_1\rangle = 1; \quad \langle\psi_2|E_2|\psi_2\rangle = 1. \tag{2.99}$$

$\sum_i E_i = I$ なので $\sum_i\langle\psi_1|E_i|\psi_1\rangle = 1$ である．$\langle\psi_1|E_1|\psi_1\rangle = 1$ なので $\langle\psi_1|E_2|\psi_1\rangle = 0$，したがって $\sqrt{E_2}|\psi_1\rangle = 0$ でなければばならない．$|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\varphi\rangle$ と分解するとする．ここで $|\varphi\rangle$ は $|\psi_1\rangle$ に直交，$|\alpha|^2 + |\beta|^2 = 1$，$|\psi_1\rangle$ と $|\psi_2\rangle$ が直交でないので $|\beta| < 1$ である．このとき $\sqrt{E_2}|\psi_2\rangle = \beta\sqrt{E_2}|\varphi\rangle$ なので

$$\langle\psi_2|E_2|\psi_2\rangle = |\beta|^2\ \langle\varphi|E_2|\varphi\rangle \le |\beta|^2 < 1 \tag{2.100}$$

となり，これは式 (2.99) と矛盾する．ここで後ろから2番目の不等式は

$$\langle\varphi|E_2|\varphi\rangle \le \sum_i\langle\varphi|E_i|\varphi\rangle = \langle\varphi|\varphi\rangle = 1 \tag{2.101}$$

から得られる．

2.2.5　射影測定

本項では一般的な測定公理 3 の重要で特別な場合について説明する．この特殊なクラスの測定を**射影測定** (projective measurement) と呼ぶ．量子計算と量子情報の多くの応用において我々は主として射影測定を扱う．公理 2 で述べたようなユニタリー変換をする能力を備えると，射影測定は実際に一般の測定公理と**等価** (equivalent) になることがわかる．射影測定に対する測定公理の表現は一般的な公理 3 とは外面上少し違っているので，この等価性については 2.2.8 項で詳しく説明する．

射影測定:　射影測定は被測定システムの状態空間上の Hermite オペレータである**観測量** (observable) M で記述される．観測量をスペクトル分解すると，

$$M = \sum_m mP_m, \tag{2.102}$$

ここで P_m は固有値 m を持つ M の固有空間への射影オペレータである．測定で得られる結果は観測量の固有値 m に対応する．状態 $|\psi\rangle$ 測定すると結果 m を得る確率は

$$p(m) = \langle\psi|P_m|\psi\rangle \tag{2.103}$$

で与えられる．測定結果 m が得られると測定直後の量子システムの状態は次式で与えられる．

$$\frac{P_m|\psi\rangle}{\sqrt{p(m)}}. \tag{2.104}$$

射影測定は公理 3 の特別ケースとみなせる．完全性関係 $\sum_m M_m^\dagger M_m = I$ だけでなく，公理 3 の測定オペレータ M_m が直交射影オペレータの条件も満たすとする．後者の条件は M_m が Hermite オペレータ，かつ $M_m M_{m'} = \delta_{m,m'} M_m$ である．これらの制約を加えると今定義したように公理 3 は射影測定になる．

コラム 2.4: Heisenberg の不確定性原理

おそらく量子力学で最もよく知られた結果は **Heisenberg の不確定性原理**であろう．A と B を 2 つの Hermite オペレータ，$|\psi\rangle$ は量子状態とする．$\langle\psi|AB|\psi\rangle = x + iy$ とし，x, y は実数とする．$\langle\psi|[A,B]|\psi\rangle = 2iy$ と $\langle\psi|\{A,B\}|\psi\rangle = 2x$ を用いるとこの式より

$$|\langle\psi|[A,B]|\psi\rangle|^2 + |\langle\psi|\{A,B\}|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2. \tag{2.105}$$

Cauchy-Schwarz の不等式より，

$$|\langle\psi|AB|\psi\rangle|^2 \le \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle, \tag{2.106}$$

2 式を組み合わせて負でない項を落とすと，

$$|\langle\psi|[A,B]|\psi\rangle|^2 \le 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle. \tag{2.107}$$

C と D を 2 つの観測量とし，$A = C - \langle C\rangle$，$B = D - \langle D\rangle$ とおいて最後の式に代入すると，通常の形の Heisenberg の不確定性原理を得る．

$$\Delta(C)\Delta(D) \ge \frac{|\langle\psi|[C,D]|\psi\rangle|}{2}. \tag{2.108}$$

観測量 C をある「精度」$\Delta(C)$ で測定すると，D の値が $\Delta(D)$ の量だけ「乱され」てなにか上式のような不等式が成立する，という不確定性原理に関して一般によく見られる誤解には注意しなければならない．量子力学における測定が被測定システムに擾乱を与えるのは事実であるが，これが不確定性原理の内容では**決してない**．

不確定性原理の正しい解釈は次の通りである．多くの量子状態を同じ状態 $|\psi\rangle$ に用意して，これらシステムの幾つかについて測定 C を行い他について測定 D を行うと，C の結果の標準偏差 $\Delta(C)$ と D の結果の標準偏差 $\Delta(D)$ の積は上記不等式 (2.108) を満たす．

不確定性原理の例として量子状態 $|0\rangle$ について，観測量 X と Y を測定することを考える．式 (2.70) で $[X,Y]=2iZ$ であることを示したので，不確定性原理より

$$\Delta(X)\Delta(Y) \geq \langle 0|Z|0\rangle = 1. \tag{2.109}$$

直接計算すればわかるように，この基本的結果の 1 つは $\Delta(X)$ と $\Delta(Y)$ は 0 よりも厳密に大きくなければならないことである．

射影測定は多くの有効な性質を持っている．特に射影測定の平均値を計算するのが容易である．測定の平均値は定義により次式で与えられる（確率論の結果の基本的定義に関しては付録 A 参照）．

$$\mathbf{E}(M) = \sum_m m\, p(m) \tag{2.110}$$

$$= \sum_m m\langle\psi|P_m|\psi\rangle \tag{2.111}$$

$$= \langle\psi|\Big(\sum_m mP_m\Big)|\psi\rangle \tag{2.112}$$

$$= \langle\psi|M|\psi\rangle. \tag{2.113}$$

これは便利な式であり，これによって多くの計算が簡単になる．観測量 M の平均値は $\langle M\rangle \equiv \langle\psi|M|\psi\rangle$ と書ける．この平均値の式から M の観測に伴う標準偏差の式が得られる．

$$[\Delta(M)]^2 = \langle (M - \langle M \rangle)^2 \rangle \tag{2.114}$$

$$= \langle M^2 \rangle - \langle M \rangle^2. \tag{2.115}$$

標準偏差は M を測定する際の観測値の典型的な広がりの尺度である．特に準備された状態 $|\psi\rangle$ に関して観測量 M を測定する実験を多数回行うと，観測値の標準偏差は $\Delta(M) = \sqrt{\langle M^2 \rangle - \langle M \rangle^2}$ で決められる．観測量で表した測定と標準偏差のこの表式から，**Heisenberg の不確定性原理** (Heisenberg uncertainty principle) のような結果が手際良く得られる（コラム 2.4 参照）.

演習 2.58: 対応する固有値 m を有する観測量 M の固有状態 $|\psi\rangle$ の量子システムを準備する．M の平均観測値と標準偏差は何か？

2 つの広く使われる測定用語を強調しておきたい．射影測定を記述する観測量を与える代わりに，単に $\sum_m P_m = I$ と $P_m P_{m'} = \delta_{mm'} P_m$ の関係を満たす直交射影オペレータ P_m の完全集合が与えられることがしばしばある．この用法に隠れた対応観測量は $M = \sum_m m P_m$ である．もう 1 つの広く使われる言葉は「基底 $|m\rangle$ での測定」である．ここで $|m\rangle$ は正規直交基底であり，この測定は単純に射影オペレータ $P_m = |m\rangle\langle m|$ で射影測定を行うことを意味する．

単一 q ビットの射影測定の例を見てみよう．最初は観測量 Z の測定である．これは固有値 $+1, -1$，対応する固有ベクトル $|0\rangle, |1\rangle$ を有する．したがって，例えば状態 $|\psi\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ について測定 Z を行えば確率 $\langle\psi|0\rangle\langle 0|\psi\rangle = 1/2$ で結果 $+1$，同様に確率 $1/2$ で結果 -1 を得る．一般に $\vec{v}$ が任意の実数の 3 次元単位ベクトルとすると次の観測量を定義できる．

$$\vec{v} \cdot \vec{\sigma} \equiv v_1 \sigma_1 + v_2 \sigma_2 + v_3 \sigma_3. \tag{2.116}$$

この観測量の測定は歴史的理由により「$\vec{v}$ 軸に沿ったスピンの測定」と呼ばれる．次の 3 つの演習で基本的で重要なこの測定の性質を確かめて欲しい．

演習 2.59: q ビットが状態 $|0\rangle$ にあるとして観測量 X を測定する．X の平均値と標準偏差は何か？

演習 2.60: $\vec{v} \cdot \vec{\sigma}$ が固有値 ± 1 を持つこと，および対応する固有空間への射影ベクトルは $P_{\pm} = (I \pm \vec{v} \cdot \vec{\sigma})/2$ で与えられることを示せ．

演習 2.61: 測定前の状態が $|0\rangle$ であるとして，$\vec{v}\cdot\vec{\sigma}$ の測定で結果 $+1$ を得る確率を求めよ．$+1$ が得られた測定後のシステムの状態は何か？

2.2.6 POVM 測定

量子測定の公理 3 は 2 つの要素を含んでいる．第 1 に測定の統計 — 異なる測定結果それぞれの確率 — を記述するルールを与える．第 2 に測定後のシステム状態を記述するルールを与える．しかし，ある種の応用では測定後のシステム状態にあまり興味がなく，各測定結果の確率が主な関心事であることがある．例えば実験結果を求めてシステムを 1 回だけ測定する実験の場合である．そのような場合，とりわけ測定の解析に適した **POVM 形式** (POVM formalism) という数学的ツールがある．(POVM は「正値オペレータ測定」(positive operator-valued measure) の略称であるが，この術語の歴史的起源について気にしなくてもよい.）この形式は公理 3 で導入された測定の一般的記述の単なる帰結であるが，POVM 理論はすっきりしていて広く使われるので，ここで改めて議論する価値がある．

状態 $|\psi\rangle$ にある量子システムについて，測定オペレータ M_m で記述される測定を行うとする．測定結果 m を得る確率は $p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$ で与えられる．次式で E_m を定義する．

$$E_m = M_m^\dagger M_m. \tag{2.117}$$

公理 3 と線形代数の初歩的計算より，E_m は $\sum_m E_m = I$ および $p(m) = \langle\psi|E_m|\psi\rangle$ を満たす正のオペレータである．したがって，オペレータ集合 E_m があれば異なる測定結果の確率を決めることができる．オペレータ E_m は測定に関する **POVM 要素** (POVM element)，完全集合 $\{E_m\}$ を **POVM** と呼ぶ．

POVM の例として測定オペレータ P_m で記述される射影測定を考える．ここで P_m は $P_m P_{m'} = \delta_{mm'} P_m$ と $\sum_m P_m = I$ を満たす射影オペレータである．この事例では（この事例だけは），$E_m \equiv P_m^\dagger P_m = P_m$ なので全 POVM 要素が測定オペレータそれ自身に等しい．

演習 2.62: 測定オペレータが POVM と一致する測定は射影測定であることを示せ．

POVM は正で $\sum_m E_m = I$ を満たすことを述べた．今 $\{E_m\}$ が $\sum_m E_m = I$ を満たす任意の集合であるとするとき，POVM $\{E_m\}$ で記述される測定を定義する測定オペレータ集合 M_m が存在することを示そう．$M_m \equiv \sqrt{E_m}$ を定義すると $\sum_m M_m^\dagger M_m = \sum_m E_m = I$，したがって集合 $\{M_m\}$ は POVM$\{E_m\}$ による測定を記述する．この理由により POVM は次の条件を満たす任意のオペレータ集合 $\{E_m\}$ として**定義**するのが便利である．(a) 各オペレータが正である．(b) 確率の和が 1 になることを示す**完全性関係** $\sum_m E_m = I$ を満たす．POVM の説明の最後に，POVM $\{E_m\}$ が与えられると，測定結果 m の確率は $p(m) = \langle\psi|E_m|\psi\rangle$ で与えられることをもう一度述べておく．

POVM の用法例として正の測定を見てきたが，それが目新しいものでなかったので特に興奮するものではなかった．次の複雑な例では POVM 形式が量子計算と量子情報における我々の直観を導く役割をすることがわかる．Alice が Bob に 2 つの状態 $|\psi_1\rangle = |0\rangle$, $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ のどちらかに準備された q ビットを与えるとする．2.2.4 項で説明したように，Bob は彼が貰ったのは $|0\rangle$ か $|1\rangle$ かを完全に信頼度良く決めることは不可能である．しかし，あるときには誤りを決して犯さずに状態を識別する測定を行うことが可能である．3 つの要素を持つ POVM を考える．

$$E_1 \equiv \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1|, \tag{2.118}$$

$$E_2 \equiv \frac{\sqrt{2}}{1+\sqrt{2}} \frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2}, \tag{2.119}$$

$$E_3 \equiv I - E_1 - E_2. \tag{2.120}$$

これらが完全性条件 $\sum_m E_m = I$ を満たす正のオペレータであり，したがって正当な POVM であることが直接証明できる．

仮に Bob に状態 $|\psi_1\rangle = |0\rangle$ が与えられたとする．彼は POVM $\{E_1, E_2, E_3\}$ で記述される測定を行う．$\langle\psi_1|E_1|\psi_1\rangle = 0$ が満たされるように E_1 をうまく選んだので，E_1 の結果を得る確率は 0 である．したがって，もし測定結果が E_1 ならば，Bob は受け取った状態が $|\psi_2\rangle$ であったと結論付けて間違いはない．同じ論法でもし測定結果が E_2 ならば，Bob が受け取ったのは状態 $|\psi_1\rangle$ であったとに違いないのが示せる．しかし時には Bob は測定結果 E_3 を得るであろうが，このときには受け取った状態を見分けることに関して何も推論できない．肝心な点

は Bob が受け取った状態の同定を **決して**誤らないことである．Bob はときどき状態同定に関する情報が全く得られないことがあるという代償のもとに，この絶対的確実性を得るのである．

この簡単な例は測定の統計のみが重要である場合に，量子測定の見通しを得る簡単で直観的な方法として，POVM 形式が便利であることを示している．後で示す例では測定結果の統計に関心を払うことが多く，したがってそこでは公理 3 で述べた一般的な測定形式よりむしろ POVM が用いられる．

演習 2.63: 測定オペレータ M_m で記述される測定を想定する．$M_m = U_m\sqrt{E_m}$ なるユニタリーオペレータ U_m が存在することを示せ．ここで E_m は測定に関する POVM である．

演習 2.64: 線形独立な状態 $|\psi_1\rangle, \ldots, |\psi_m\rangle$ の中から選ばれた量子状態が 1 つ Bob に与えられるとする．測定結果 E_i, $1 \le i \le m$ が得られれば Bob に与えられたのが $|\psi_i\rangle$ であると確信をもってわかるような POVM を構築せよ．(POVM は各 i に対して $\langle\psi_i|E_i|\psi_i\rangle > 0$ でなければならない．)

コラム 2.5: 一般的測定，射影測定および POVM

多くの量子力学入門書には射影オペレータしか書かれていないので，2.2.6 項で述べた POVM 形式はもとより，公理 3 で述べた測定の一般的議論は多くの物理学者に馴染みが少ないかも知れない．多くの物理学者が一般測定形式について学ばない理由は，多くの物理システムが十分な精度で測定されないからである．量子計算と量子情報では，なし得る測定をこのうえなく精密に制御することを目指しており，測定を記述する包括的形式が必要になる．

もちろん他の量子力学の公理を考えに入れると，ユニタリー演算で拡張された射影測定は 2.2.8 項で示したように一般の測定と完全に**等価**である．そこで射影測定を使い慣れている物理学者はどんな目的で一般形式である公理 3 から出発するのかという疑問を持つかも知れない．こうするには幾つかの理由がある．第 1 に数学上一般的測定は測定オペレータへの制約が少ないので，ある意味で射影測定よりも簡単である．例えば射影測定における $P_iP_j = \delta_{ij}P_i$ のような条件は一般測定の要件にはない．この構造のほうが簡単なので一般

測定には射影測定にない多くの便利な性質が生まれる．第 2 に量子計算と量子情報には — 例えば量子状態の集合を識別する最適手法というような — 答えるには射影測定ではなく一般的測定が必要になるような重要な問題が存在する．

出発点として公理 3 を選ぶ第 3 の理由は**再現性** (repeatability) と呼ばれる射影測定の性質に関連している．射影測定には一度射影測定を行い結果 m を得ると，その測定を繰り返しても再び結果 m を与え状態は変化しないという意味で，再現性がある．これをみるのに $|\psi\rangle$ を初期状態とする．最初の測定後の状態は $|\psi_m\rangle = \bigl(P_m|\psi\rangle\bigr)/\sqrt{\langle\psi|P_m|\psi\rangle}$ となる．P_m を $|\psi_m\rangle$ に適用しても変化は生じないので $\langle\psi_m|P_m|\psi_m\rangle = 1$ となり，したがって繰り返し測定してもそのたびに結果 m を与えて状態は変化しない．

射影測定のこの再現性をみると，量子力学の多くの重要な測定が射影測定でないという事実を教えてくれる．例えば光子の位置を測定するのにもし銀メッキスクリーンを用いるとその過程で光子は壊れてしまう．これでは光子の位置測定を繰り返すことは不可能になる！ 多くの他の量子測定も射影測定と同じ意味では再現可能ではない．そのような測定には一般測定公理である公理 3 を採用しなければならない．この描像で POVM は何処に位置するのか？ POVM は一般測定形式の特別な場合と見なされ，測定後の状態を知る必要がないときに，一般測定の統計を知ることができる最も簡単な手法を提供してくれる．それは量子測定に格別な見通しを与える便利な数学的手法である．

2.2.7 位 相

「位相」は量子力学で普通に使われる言葉であるが，文脈によって幾つか異なる意味を持っている．ここでは 2 つの意味を考える．例えば $|\psi\rangle$ を状態ベクトル，θ を実数として状態 $e^{i\theta}|\psi\rangle$ を考える．我々は状態 $e^{i\theta}|\psi\rangle$ は**グローバル位相因子** (global phase factor) $e^{i\theta}$ を除いて $|\psi\rangle$ に等しいという．これら 2 つの状態に対して予想される**測定の統計** (statistics of measurement) が同じになることは興味深い．これを確かめるためにある量子測定に関する測定オペレータ

を M_m とすると，各々において測定結果 m を得る確率は $\langle\psi|M_m^\dagger M_m|\psi\rangle$ および $\langle\psi|e^{-i\theta}M_m^\dagger M_m e^{i\theta}|\psi\rangle = \langle\psi|M_m^\dagger M_m|\psi\rangle$ である．したがって，観測の観点からこれら 2 つの状態は同一である．この理由で我々はグローバル位相因子は物理システムの観測される性質に無関係であるとしてこれを無視する．

相対位相 (relative phase) と呼ぶ別の種類の位相があり，これは全く違う意味を持っている．2 つの状態を考える．

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \quad \frac{|0\rangle-|1\rangle}{\sqrt{2}}. \tag{2.121}$$

第 1 の状態では $|1\rangle$ の振幅は $1/\sqrt{2}$，第 2 の状態では $-1/\sqrt{2}$ である．各々の場合に振幅の**大きさ** (magnitude) は同じであるが正負符号が異なる．一般的に実数 θ に対して $a = \exp(i\theta)\, b$ の関係があるならば 2 つの振幅 a，b は**相対位相が異なる**という．さらに一般的にある基底における各々の振幅がそのような位相因子で関係しているならば，2 つの状態はその基底において**相対位相が異なる** という．例えば上に示した 2 つの状態は相対位相因子を除いて同じである．なぜならば $|0\rangle$ の振幅は同じ（相対位相因子は 1）であり，$|1\rangle$ の振幅は -1 の相対位相因子が異なるだけである．相対位相因子とグローバル位相因子の相違は，相対位相では位相因子が振幅毎に変化することにある．これによりグローバル位相と異なり相対位相は基底に依存する．その結果，ある基底で相対位相のみが異なる状態は，測定の統計において物理的に観測し得る違いを生むので，グローバル位相が異なる場合と違って，これらの状態を物理的に等価と見なすことはできない．

演習 2.65: 状態 $(|0\rangle+|1\rangle)/\sqrt{2}$ と $(|0\rangle-|1\rangle)/\sqrt{2}$ が相対位相を除いて同じでないような基底で表せ．

2.2.8　複合システム

2 つ（あるいはそれ以上）の異なる物理システムからなる複合量子システム (composite quantum system) を考える．複合システムの状態を記述するにはどうすればよいか？ 次の公理は要素システムの状態空間から，複合システムの状態空間を構築する方法について述べる．

公理 4: 複合物理システムの状態空間は要素物理システムの状態空間のテンソル積で与えられる．さらに 1 から n までの番号を持つシステムがあり，i 番目のシステムが $|\psi_i\rangle$ の状態にあるとき，これらを要素システムとする全システムの複合状態は $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$ である．

なぜテンソル積が複合物理システムを記述する数学的構造なのか？ ある段階ではより基本的な何かに還元せずに，それを基本公理として受け入れて先に進むことができる．最後には量子力学で複合システムを記述する**何か正統的な方法** があると我々は期待する．この公理に到達できる他の方法があるだろうか？ ここに示すのは（導出ではなく）よく使われる発見的方法の 1 つである．物理学者はよく**量子力学の重ね合せ原理**について述べる．その内容は，もし $|x\rangle$ と $|y\rangle$ が量子システムの 2 つの状態ならば，任意の重ね合せ $\alpha|x\rangle + \beta|y\rangle$（ただし $|\alpha|^2 + |\beta|^2 = 1$）も量子システムの許された状態である．複合システムではもし $|A\rangle$ がシステム A の状態，$|B\rangle$ がシステム B の状態であるなら，合わさったシステム AB にも何か対応する状態があり，それをとりあえず $|A\rangle|B\rangle$ と書く．この形の積状態に重ね合せ原理を適用すると，上に述べたテンソル積の公理に行き着く．我々は重ね合せ原理を量子力学を記述する基本部分と見なしていないのでこれは導出ではないが，これらの概念を再構成するいろいろな方法の雰囲気を感じてもらえるであろう．

文献には複合システムを記述するさまざまな記号が現れる．このように増えた理由の一部は異なる記号が異なる応用により適合するからであり，我々も時に応じて特別の記号を導入するのが便利なことがあろう．この時点では文脈から判断できないときに，異なるシステムの状態やオペレータを表す便利な添字記号について述べておけば十分であろう．例えば 3 つの q ビットを含むシステムにおいて X_2 は第 2 の q ビットに働く Pauli の σ_x オペレータを表す．

演習 2.66: 状態 $(|00\rangle + |11\rangle)/\sqrt{2}$ にある 2 個の q ビットシステムに対する観測量 $X_1 Z_2$ の平均値は 0 であることを示せ．

ユニタリーダイナミックスを伴う射影測定があれば，一般測定を行うのに十分であることを 2.2.5 項で述べた．これは複合量子システム用いて証明することができ，上記の公理 4 の良い例題になる．状態空間 Q の量子システムがあるとして

このシステム Q について測定オペレータ M_m で記述される測定を行う．この際に状態空間 M をもつ**補助システム** (ancilla systm) を導入する．この状態空間 M は我々が適用したい測定で得られる可能性のある結果に 1 対 1 に対応した，正規直交基底 $|m\rangle$ を有する．この補助システムは構築中に現れる単なる数学的便法と考えてもよいし，要求される性質を備えた状態空間を有するもう 1 つの量子システムを問題に導入したものと解釈することもできる．

$|0\rangle$ を M の任意の固定した状態とし，Q の状態 $|\psi\rangle$ と状態 $|0\rangle$ の積 $|\psi\rangle|0\rangle$ に働くオペレータを次式で定義する．

$$U|\psi\rangle|0\rangle \equiv \sum_m M_m|\psi\rangle|m\rangle. \tag{2.122}$$

状態 $|m\rangle$ の直交性と完全性関係 $\sum_m M_m^\dagger M_m = I$ を用いると，U は $|\psi\rangle|0\rangle$ の形の状態間の内積を保存する．

$$\begin{aligned}\langle\varphi|\langle 0|U^\dagger U|\psi\rangle|0\rangle &= \sum_{m,m'} \langle\varphi|M_m^\dagger M_{m'}|\psi\rangle\langle m|m'\rangle & (2.123)\\ &= \sum_m \langle\varphi|M_m^\dagger M_m|\psi\rangle & (2.124)\\ &= \langle\varphi|\psi\rangle. & (2.125)\end{aligned}$$

演習 2.67 の結果より U は空間 $Q \otimes M$ 上のユニタリーオペレータに拡張できて，これも U と表記する．

演習 2.67: V は部分空間 W を含む Hilbert 空間であるとする．$U : W \to V$ は内積を保存する線形オペレータとする．つまり W における任意の $|w_1\rangle$ と $|w_2\rangle$ に対して

$$\langle w_1|U^\dagger U|w_2\rangle = \langle w_1|w_2\rangle. \tag{2.126}$$

U を**拡張**するユニタリーオペレータ $U' : V \to V$ が存在することを証明せよ．つまり W 中のすべての $|w\rangle$ に対して $U'|w\rangle = U|w\rangle$ であるが U' は全空間 V 上で定義される．通常拡大を表すプライム記号「$'$」を省略して単に U と書く．

U を $|\psi\rangle|0\rangle$ に作用させた後で，射影オペレータ $P_m \equiv I_Q \otimes |m\rangle\langle m|$ で記述される射影測定を 2 つのシステムに適用すると考える．結果 m を得る確率は公理 3

で与えられたように

$$p(m) = \langle\psi|\langle 0|U^\dagger P_m U|\psi\rangle|0\rangle \tag{2.127}$$

$$= \sum_{m',m''} \langle\psi|M_{m'}^\dagger \langle m'|(I_Q \otimes |m\rangle\langle m|)M_{m''}|\psi\rangle|m''\rangle \tag{2.128}$$

$$= \langle\psi|M_m^\dagger M_m|\psi\rangle. \tag{2.129}$$

測定結果 m を得た後のシステム QM の結合状態は次式で与えられる．

$$\frac{P_m U|\psi\rangle|0\rangle}{\sqrt{\langle 0|\langle\psi|U^\dagger P_m U|\psi\rangle|0\rangle}} = \frac{M_m|\psi\rangle|m\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{2.130}$$

したがって，測定後のシステム M の状態は $|m\rangle$ であり，システム Q の状態は公理 3 で述たように

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{2.131}$$

したがって，ユニタリー時間発展，射影測定，補助システムの導入能力を合わせると，公理 3 で述べた如何なる形の測定でも実現できる．

公理 4 を用いると複合量子システムに伴う最も興味深く，かつ最もわかりにくい概念の 1 つである**もつれ** (entanglement) の定義も可能になる．2 つの q ビットシステムを考える．

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.132}$$

この状態は顕著な特徴を持っており $|\psi\rangle = |a\rangle|b\rangle$ となるような単一 q ビット状 態 $|a\rangle, |b\rangle$ が存在しない．この事実を次の演習で納得してもらいたい．

演習 2.68: すべての単一 q ビット状態 $|a\rangle, |b\rangle$ に対して $|\psi\rangle \neq |a\rangle|b\rangle$ を証明せよ．

この（要素システムの状態の積として書けないという）性質を持つ複合システムの状態を**もつれ状態** (絡み合い状態，entangled state) と呼ぶ．理由は誰も十分理解していないが，もつれ状態は量子計算と量子情報において重要な役割を果たし，今後本書で繰り返し出てくる．すでに 1.3.7 項で述べたように，もつれは量子テレポーテーションで重要な役割を果たす．本章ではもつれによって可能となる奇妙な効果の例 — 超高密度符号化（2.3 節）と Bell の不等式の破綻（2.6 節）の 2 つ — を紹介する．

2.2.9 量子力学：全体の展望

これまでに量子力学の基本公理をすべて説明した．本書ではこの後これら公理から得られる結果を取り上げていく．この公理を手早く振り返り全体展望の中の位置づけを見てみよう．

公理 1 は孤立した量子システムを記述する方法を明記して，量子力学の舞台を設定する．公理 2 は**閉じた** (closed) 量子システムのダイナミックスが Schrödinger 方程式，したがってユニタリー時間発展で記述されることを教えている．公理 3 は測定を記述する処方箋を与えて，量子システムから情報を取り出す方法を示している．公理 4 は個別の量子システムの状態空間を結合して，複合システムを記述する方法を教えている．

少なくとも古典的観点から量子力学が奇妙だと思われるのは，我々が状態ベクトルを直接観測できないことである．それはあたかも盤上の駒の正確な位置がわからずに，升目のならびだけの知識でチェスのゲームを行うのに似ている．古典物理学 — と我々の直観 — が教えるところでは，エネルギー，位置，速度のような対象の基本的性質は直接観測できる．量子力学ではこれらの量はもはや基本的とは見なされず，我々が直接観測できない状態ベクトルがその位置を占める．それはあたかも量子力学には**隠れた世界** (hidden world) があって，我々は間接かつ不完全にしか近づけないように見える．さらに古典的システムでは，観測するだけなら状態変化を起こすことはない．ボールを見るたびにその位置が変化するなら，テニスはどれほど難しいゲームになるだろうか？ しかし公理 3 によれば量子力学の観測は一般にシステム状態を変化させる侵襲的手続きである．

量子力学のこの奇妙な特徴からどのような結論を引き出すか？ 数学的に等価な方法で量子力学を古典物理学に似た構造に再構成することは可能か？ 2.6 節ではそのような再構成の試みの失敗を運命付ける驚くべき結果である **Bell の不等式** (Bell's inequality) を証明する．我々は量子力学の非直観性につきまとわれている．もちろんそれに相応しい見返りは悲しみではなく喜びである！ 量子力学を直観的にする理論的ツールを作る機会を与えてくれる．さらに古典的世界の可能性の限界を超えて情報処理を行うために，状態ベクトルの隠れた性質を利用することができる．この非直観的振る舞いがなければ，量子計算と量子情報への興味は失われてしまう．

ここで話を変えて次の自問をしてみる.「もし量子力学が古典物理学とそれほど違っているのなら，日常世界が古典的に見えるのはなぜか？」日常生活で隠れた状態ベクトルの証拠が全然見えないのはなぜか？ 我々が見る — 日常出会う時間，長さ，質量のスケールで成立する — 古典的世界は近似的記述として量子力学から導くことができる．量子力学から古典物理学が生じる詳細な説明は本書の範囲外であるが，興味を持つ読者は 8 章の最後にある「歴史と参考資料」にあるこの話題の議論を調べてほしい.

2.3 応用：超高密度符号化

簡単であるが**超高密度符号化**(superdense coding) は基本的量子力学の驚くべき応用である．そこでは前節で述べた基本的量子力学の全概念が具体的かつ有意義に組み合わされ，量子力学を用いて達成できる情報処理タスクの理想的な例となっている.

超高密度符号化には互いに遠く離れた 2 人の当事者 — 通常 Alice と Bob と呼ぶ — が含まれる．彼らのゴールは Alice から Bob へ何か古典情報を送ることである．Alice が古典情報 2 ビットを持っていてそれを Bob に送りたいが，Alice が送れるのは 1 個の q ビットだけであるとする．彼女は目的を達成できるか？

超高密度符号化が教えるところでは，この問いに対する答えは yes である．Alice と Bob が最初にもつれ状態にある一対の q ビットを共有しているとする.

$$|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \tag{2.133}$$

図 2.3 に示すように最初に Alice は第 1 の q ビットを所有し，一方 Bob は第 2 の q ビットを持っている．$|\psi\rangle$ は固定した状態であり，この状態を作るために Alice が Bob に何も送る必要はないことに注意する．その代わりにあらかじめ第 3 者がもつれ状態を作って q ビットの一方を Alice に他方を Bob に送ったものでもよい.

Alice は持っている単一 q ビットを Bob に送ることにより，古典情報 2 ビットを Bob と通信できることがわかる．彼女が使う手続きはこうである： もしビット列「00」を送りたいならば彼女は q ビットに何もしない．「01」を送りたければ彼女の q ビットに位相反転 Z を施す．「10」を送りたければ量子 NOT ゲートを

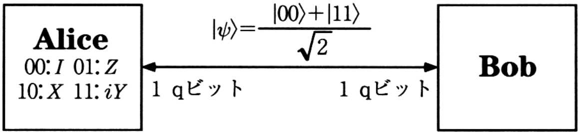


図 **2.3:** 超高密度符号化の初期構成．Alice と Bob はそれぞれもつれ合った一対の q ビットの半分を持っている．Alice は超高密度符号化によりあらかじめ共有したもつれと単一 q ビットのみを用いて古典情報 2 ビットを Bob に送ることができる．

適用する．「11」を送りたければ iY ゲートを施す．この結果生じる状態は容易に求められる：

$$00: \ |\psi\rangle \to \frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.134}$$

$$01: \ |\psi\rangle \to \frac{|00\rangle - |11\rangle}{\sqrt{2}} \tag{2.135}$$

$$10: \ |\psi\rangle \to \frac{|10\rangle + |01\rangle}{\sqrt{2}} \tag{2.136}$$

$$11: \ |\psi\rangle \to \frac{|10\rangle - |01\rangle}{\sqrt{2}} \tag{2.137}$$

1.3.6 項で見たようにもつれの新規性を最初に認めた先駆者達に敬意を表して，これらの 4 状態は **Bell 基底** (Bell basis)，**Bell 状態** (Bell state) または **EPR 対** (EPR pair) 等と呼ぶ．Bell 状態は正規直交基底を形成するので，適切な量子測定により識別できる．もし Alice が彼女の q ビットを Bob に送って Bob に 2 つの q ビットを持たせると，Bob は Bell 基底で測定を行うことにより可能な 4 つのビット列のうちで Alice がどれを送ったかを決めることができる．

まとめると Alice は単一 q ビットだけと相互作用をすることにより，Bob に 2 ビットの情報を送ることができる．もちろん手順には 2 つの q ビットが含まれているが，Alice は第 2 の q ビットと相互作用する必要は全くない．12 章 (第 III 巻) で見るように古典的には，Alice が行うタスクは 1 個の古典ビットを送るのでは不可能であったであろう．さらにこの注目すべき超高密度符号化は実験室で部分的に証明されている (実験的検証の論文は「歴史と参考資料」欄を参照)．後の章で見るように量子力学により情報処理を行う他の多くの例の中には，超高密度符号化よりもっと目覚ましいものが幾つかある．しかし重要な点はこの美しい例の中にすでに現れている：情報は物理的であり量子力学のような驚くべき物理学

理論によって，驚くべき情報処理の可能性が予言されるかも知れない．

演習 2.69: Bell 基底が 2 個の q ビット空間の直交基底を形成することを証明せよ．

演習 2.70: Alice が持つ q ビットに働く任意の正のオペレータを E とする．$|\psi\rangle$ が任意の 4 つの Bell 状態であるとき，$\langle\psi|E\otimes I|\psi\rangle$ **は同じ値をとる**ことを示せ．超高密度符号化手順において，Bob に送る途中の Alice の q ビットをある悪意を持つ第 3 者（「Eve」）が横取りしたとする．Eve は Alice が送ろうとしたのは，4 つのビット列 00, 01, 10, 11 のどれかについて何か推論できるか？ もしできるなら，あるいはもしできないならそれはなぜか？

2.4 密度オペレータ

我々は状態ベクトルの言葉を使って量子力学を定式化してきた．これとは別に**密度オペレータ** (density operator) もしくは**密度行列** (density matrix) と呼ぶ新たなツールを用いて定式化することもできる．このもう 1 つの定式化は，数学的には状態ベクトルによるアプローチと等価であるが，量子力学において通常出会う幾つかのケースを考えるのに便利な言語が提供できる．次の 3 節では量子力学の密度オペレータ形式について述べる．2.4.1 節で量子状態のアンサンブルの概念を用いて密度オペレータを導入する．2.4.2 項では密度オペレータの一般的性質を明らかにする．最後に 2.4.3 項では密度オペレータが持つ際だった応用 — 複合システムにおける**個別の部分システム**を記述するツール — について述べる．

2.4.1 量子状態のアンサンブル

密度オペレータの言語は，状態が全くわからない量子システムを記述する便利な方法を提供する．正確に言えば量子システムが多くの状態 $|\psi_i\rangle$（i は指数）の 1 つにあるとして，その各々の確率を p_i とする．$\{p_i, |\psi_i\rangle\}$ を**純粋状態のアンサンブル** (ensemble of pure state) と呼ぶ．このシステムの密度オペレータを次式で定義する．

$$\rho \equiv \sum_i p_i |\psi\rangle\langle\psi_i|. \tag{2.138}$$

密度オペレータを**密度行列** (density matrix) とも呼び，これら 2 つの言葉を区別せずに使うことにする．量子力学の全公理を密度オペレータの言葉で再構築することができる．本項と次項の目的はこの再構築の仕方を説明し，どのようなときに便利かを説明することにある．密度オペレータの言葉を使うか，状態ベクトルの言葉を使うかは両方とも同じ結果を与えるので趣味の問題である．しかしある視点からアプローチするほうが他の視点よりはるかに易しいことがある．

例えば，閉じた量子システムの時間発展を，ユニタリーオペレータ U で記述するとする．もしシステムの初期状態が $|\psi_i\rangle$，その確率が p_i ならば時間発展後の状態は $U|\psi_i\rangle$，その確率は p_i である．したがって密度オペレータの時間発展は次式で記述される．

$$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i| \xrightarrow{U} \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^\dagger = U\rho U^\dagger. \tag{2.139}$$

測定も密度オペレータで容易に記述できる．測定オペレータ M_m で記述される測定を行うとする．初期状態が $|\psi_i\rangle$ なら，結果 m を得る確率は

$$p(m|i) = \langle\psi_i|M_m^\dagger M_m|\psi_i\rangle = \mathrm{tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|), \tag{2.140}$$

ここで最後の等式を得るのに式 (2.61) を用いた．全確率の法則（この説明および確率論の基本的記号は付録 A 参照）より，結果 m を得る確率は，

$$\begin{aligned} p(m) &= \sum_i p(m|i)p_i & (2.141)\\ &= \sum_i p_i \mathrm{tr}(M_m^\dagger M_m|\psi_i\rangle\langle\psi_i|) & (2.142)\\ &= \mathrm{tr}(M_m^\dagger M_m\rho). & (2.143)\end{aligned}$$

測定結果 m を得た後のシステムの密度オペレータはどうなるか？ もし初期状態が $|\psi_i\rangle$ ならば，結果 m を得た後の状態は

$$|\psi_i^m\rangle = \frac{M_m|\psi_i\rangle}{\sqrt{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}}. \tag{2.144}$$

したがって，結果 m を得た後は状態 $|\psi_i^m\rangle$，対応する確率 $p(i|m)$ のアンサンブル

が得られる．したがって，これに対する密度オペレータ ρ_m は

$$\rho_m = \sum_i p(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\langle\psi_i|M_m^\dagger M_m|\psi_i\rangle}. \qquad (2.145)$$

しかし基礎的確率論より $p(i|m) = p(m,i)/p(m) = p(m|i)p_i/p(m)$．式 (2.143), (2.140) を代入すると

$$\rho_m = \sum_i p_i \frac{M_m|\psi_i\rangle\langle\psi_i|M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m\rho)} \qquad (2.146)$$

$$= \frac{M_m\rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m\rho)}. \qquad (2.147)$$

これまでに示したのは，ユニタリー時間発展と測定に関する量子力学の基本公理が，密度オペレータの言葉で言い換えられることである．この言い換えを完全なものにするために，状態ベクトルの概念に頼らずに密度行列本来の性質を次項に示す．

しかし，その前に密度オペレータに関する言葉と，もう 1 つの事実を紹介しておくのが有益であろう．最初に言葉である．状態 $|\psi\rangle$ が正確にわかっている量子システムを**純粋状態** (pure state) にあるという．この場合の密度オペレータは単に $\rho = |\psi\rangle\langle\psi|$ である．そうでなければ ρ は**混合状態** (mixed state) にあり，ρ に対するアンサンブルの異なる純粋状態の**混合**であるという．演習で状態が純粋か混合かを決める簡単な評価基準を示すよう求められる．純粋状態は $\mathrm{tr}(\rho^2) = 1$ を満たし，混合状態は $\mathrm{tr}(\rho^2) < 1$ である．術語に関して一言いうと「混合状態」という言葉で純粋状態と混合状態をひっくるめて表すことがある．この語法の起源は状態が純粋とは必ずしも**仮定**していないことを意味しているようである．第 2 に「純粋状態」は密度オペレータ ρ と区別して状態ベクトル $|\psi\rangle$ を指すのにしばしば用いられる．

最後に確率 p_i を持つ状態 ρ_i の量子システムを準備したとする．このシステムの密度行列が $\sum_i p_i\rho_i$ で記述できることは容易に納得できる．この証明には ρ が純粋状態のアンサンブル $\{p_{ij}, |\psi_{ij}\rangle\}$ （i は固定）から作られるとすると，状態

$|\psi_{ij}\rangle$ にある確率は $p_i p_{ij}$ である．システムの密度行列は

$$\rho = \sum_{ij} p_i p_{ij} |\psi_{ij}\rangle\langle\psi_{ij}| \tag{2.148}$$

$$= \sum_i p_i \rho_i, \tag{2.149}$$

ここで定義 $\rho_i = \sum_j p_{ij}|\psi_{ij}\rangle\langle\psi_{ij}|$ を用いた．ρ は確率 p_i を有する状態 ρ_i の混合であるという．混合の概念は量子雑音のような問題の解析に繰り返し現れる．量子雑音では雑音により量子状態に関する我々の知識が失われる効果が生じる．簡単な例として，上で述べた測定シナリオにおいて，何らかの理由で測定結果 m が失われるとする．量子状態は確率 $p(m)$ で状態 ρ_m にあるであろうが，実際の m の値はもはやわからない．したがって，そのような量子システムの状態は密度オペレータで記述される．

$$\rho = \sum_m p(m)\rho_m \tag{2.150}$$

$$= \sum_m \mathrm{tr}(M_m^\dagger M_m \rho) \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)} \tag{2.151}$$

$$= \sum_m M_m \rho M_m^\dagger, \tag{2.152}$$

これは簡潔な式でありシステムの演算をさらに解析する出発点となる．

2.4.2 密度オペレータの一般的性質

密度オペレータは量子状態のアンサンブルを記述する手段として導入された．本項ではこの記述から離れてアンサンブルの解釈に頼らずに，密度オペレータ固有の性質を明らかにする．これによって状態ベクトルに基礎を置かずに，量子力学を記述する我々の計画が完成する．また，この機会を利用して密度オペレータの多くの基礎的性質を明らかにする．

密度オペレータの性質は次の便利な定理で示される．

定理 2.5:（密度オペレータの特性）　オペレータ ρ がアンサンブル $\{p_i, |\psi_i\rangle\}$ に伴う密度オペレータであるのは，次の条件が満たされるときのみである．

(1) **（トレースの条件）**　ρ は 1 に等しいトレースを持つ．

(2) **（正の条件）**　ρ は正のオペレータである．

証明　$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ が密度オペレータであるとする．このとき

$$\mathrm{tr}(\rho) = \sum_i p_i \mathrm{tr}(|\psi_i\rangle\langle\psi_i|) = \sum_i p_i = 1, \tag{2.153}$$

したがって，トレース条件 $\mathrm{tr}(\rho) = 1$ は満たされる．$|\varphi\rangle$ が状態空間の任意のベクトルであるとすると，

$$\langle\varphi|\rho|\varphi\rangle = \sum_i p_i \langle\varphi|\psi_i\rangle\langle\psi_i|\varphi\rangle \tag{2.154}$$

$$= \sum_i p_i |\langle\varphi|\psi_i\rangle|^2 \tag{2.155}$$

$$\geq 0, \tag{2.156}$$

したがって，正の条件も満たされる．

逆に ρ がトレースと正の条件を満たす任意のオペレータとする．ρ が正なのでスペクトル分解ができる．

$$\rho = \sum_i \lambda_j |j\rangle\langle j|, \tag{2.157}$$

ここでベクトル $|j\rangle$ は直交，λ_j は の実数で負でない ρ の固有値である．トレース条件より $\sum_j \lambda_j = 1$ がわかる．したがって，確率 λ_j で状態 $|j\rangle$ にあるシステムは密度行列 ρ を持つ．つまりアンサンブル $\{\lambda_j, |j\rangle\}$ は密度オペレータ ρ を生成する状態のアンサンブルである．　□

この定理は密度オペレータ固有の性質を示している：つまり密度オペレータはトレースが 1 に等しい正のオペレータ ρ であるとして**定義**できる．この定義により我々は量子力学の公理を密度オペレータ描像で再構築できる．参照しやすいように再構築した公理をすべてここに記しておく．

公理 1: 任意の孤立した物理システムに関連してシステムの**状態空間**と呼ぶ内積を持つ複素ベクトル空間（つまり Hilbert 空間）が存在する．そのシステムはトレースが 1 に等しい正のオペレータである**密度オペレータ**ρ で完全に

記述される．もし量子システムが確率 p_i で状態 ρ_i にあるならばシステムの密度オペレータは $\sum_i p_i\rho_i$ である．

公理 2: **閉じた**量子システムの時間発展は**ユニタリー変換**で記述される．つまり，時刻 t_1 におけるシステムの状態 ρ は，時刻 t_2 におけるシステムの状態 ρ' と，時刻 t_1 と t_2 にのみ依存するユニタリーオペレータ U によって与えられる．

$$\rho' = U\rho U^\dagger. \tag{2.158}$$

公理 3: 量子測定は**測定オペレータ**の集まり $\{M_m\}$ によって記述される．これらは被測定システムの状態空間に働くオペレータである．指数 m は実験で得られる測定結果を指す．もし測定直前の量子システムの状態が ρ ならば，結果 m が得られる確率は

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \rho) \tag{2.159}$$

であり，測定後の状態は

$$\frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)} \tag{2.160}$$

である．測定オペレータは**完全性の式**を満たす．

$$\sum_m M_m^\dagger M_m = I. \tag{2.161}$$

公理 4: 複合物理システムの状態空間は，その要素である物理システムの状態空間のテンソル積で与えられる．要素システムに 1 から n までの番号を付け i 番目の状態を ρ_i とすると，全複合システムの結合状態は $\rho_1 \otimes \rho_2 \otimes \ldots \rho_n$ である．

密度オペレータによる量子力学の基本公理の再構築は，もちろん状態ベクトルによる記述と数学的に等価である．しかし量子力学を考える方法として密度オペレータによるアプローチは 2 つの応用で際立っている．つまり状態がわからない量子システムを記述する場合と，複合量子システムの部分システムを記述する場合であり，後者については次項で説明する．本項ではこの後，密度行列の性質を詳しく述べる．

演習 2.71:（混合状態か純粋状態かを決める基準） ρ は密度オペレータとする．$\mathrm{tr}(\rho^2) \le 1$ であり，ここで等号は ρ が純粋状態のときにのみ成り立つことを示せ．

密度行列で表した量子状態のアンサンブルに関して，密度行列の固有値と固有ベクトルが何か特別の意味を持つと想像するのは，陥りやすい（そして驚くほど共通の）誤解である．例えば密度行列

$$\rho = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1| \tag{2.162}$$

は量子システムは確率 3/4 で状態 $|0\rangle$，確率 1/4 で状態 $|1\rangle$ にあるに違いないと考えるかも知れない．しかし必ずしもそうではない．仮に

$$|a\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle + \sqrt{\frac{1}{4}}|1\rangle \tag{2.163}$$

$$|b\rangle \equiv \sqrt{\frac{3}{4}}|0\rangle - \sqrt{\frac{1}{4}}|1\rangle \tag{2.164}$$

を定義する．量子システムは確率 1/2 で状態 $|a\rangle$，確率 1/2 で状態 $|b\rangle$ にある．これに対応する密度行列は容易に求められる．

$$\rho = \frac{1}{2}|a\rangle\langle a| + \frac{1}{2}|b\rangle\langle b| = \frac{3}{4}|0\rangle\langle 0| + \frac{1}{4}|1\rangle\langle 1|. \tag{2.165}$$

つまり量子状態の 2 つの**異なる**アンサンブルが**同じ**密度行列を形成している．一般に密度行列の固有ベクトルと固有値は，特定の密度行列を形成し得る多くの可能なアンサンブルの **1 つ**を示しているにすぎず，それが特別の立場にあるアンサンブルであると考える理由はない．

この議論に照らして当然出てくるのは，どのクラスのアンサンブルが特定の密度行列の元になるか？という疑問である．この問題の答えはこれから導くが，量子計算と量子情報において，とりわけ量子雑音と量子誤り訂正符号（8 章と 10 章：第 III 巻）を理解するのに，それは驚くほど多くの応用を持っている．これを解くには，必ずしも正規化されていないベクトル $|\tilde{\psi}_i\rangle$ を用いるのが便利である．集合 $|\tilde{\psi}_i\rangle$ はオペレータ $\rho \equiv \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$ を**生成**し，通常の密度オペレータのアンサンブル描像との関係は式 $|\tilde{\psi}_i\rangle = \sqrt{p_i}|\psi_i\rangle$ で表される．2 つのベクトルの集合 $|\tilde{\psi}_i\rangle$ と $|\tilde{\varphi}_i\rangle$ が同じオペレータ ρ を生成するのはどのようなときか？ この問題を解く

と，どのようなアンサンブルが与えられた密度行列を生み出すかという疑問に答えることができる．

定理 2.6:（密度行列に対するアンサンブルのユニタリーな自由度）　集合 $|\tilde{\psi}_i\rangle$ と $|\tilde{\varphi}_i\rangle$ が同じ密度行列を生成するのは，

$$|\tilde{\psi}_i\rangle = \sum_j u_{ij}|\tilde{\varphi}_j\rangle \tag{2.166}$$

のときのみである．ここで u_{ij} は指数 i, j をもつ複素数のユニタリー行列であり，ベクトル $|\tilde{\psi}_i\rangle$ と $|\tilde{\varphi}_i\rangle$ の小さいほうにはベクトル 0 を補って 2 つの集合の要素数を同じにそろえる．

この定理の結果として，あるユニタリー行列 u_{ij} に対して

$$\sqrt{p_i}|\psi_i\rangle = \sum_j u_{ij}\sqrt{q_j}|\varphi_j\rangle \tag{2.167}$$

のときにのみ，**正規化状態** (normalized state) $|\psi_i\rangle$，$|\varphi_j\rangle$ と確率分布 p_i，q_j に対して，$\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i| = \sum_i q_i|\varphi_i\rangle\langle\varphi_i|$ が成り立つ．ここで小さなアンサンブルには確率 0 の要素を補って，2 つのアンサンブルを同じサイズにする．このように定理 2.6 は与えられた密度行列を生成するアンサンブル $\{p_i, |\psi_i\rangle\}$ の自由度の特性を表す．実際，前に述べた 2 つの異なる分解を有する密度行列の例 (2.162) は，この一般則の特殊例に当たることが容易に確認できる．この定理を証明しよう．

証明　あるユニタリー u_{ij} に対して $|\tilde{\psi}_i\rangle = \sum_j u_{ij}|\tilde{\varphi}_j\rangle$ とする．このとき

$$\sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_{ijk} u_{ij}u^*_{jk}|\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \tag{2.168}$$

$$= \sum_{jk}\left(\sum_i u^\dagger_{ki}u_{ij}\right)|\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \tag{2.169}$$

$$= \sum_{jk} \delta_{kj}|\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_k| \tag{2.170}$$

$$= \sum_j |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j|, \tag{2.171}$$

これは $|\tilde{\psi}_i\rangle$ と $|\tilde{\varphi}_j\rangle$ は同じオペレータを生成することを示す．

逆に

$$A = \sum_j |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i| = \sum_j |\tilde{\varphi}_j\rangle\langle\tilde{\varphi}_j| \tag{2.172}$$

とする．状態 $|k\rangle$ は直交，λ_k は厳密に正として $A = \sum_k \lambda_k |k\rangle\langle k|$ が A に対する分解であるとする．我々の戦略は状態 $|\tilde{\psi}_i\rangle$ を状態 $|\tilde{k}\rangle \equiv \sqrt{\lambda_k}|k\rangle$ に関係付け，同様に状態 $|\tilde{\varphi}_i\rangle$ を $|\tilde{k}\rangle$ に関係づけることとする．この 2 つを組み合わせると望む結果が得られる．$|\psi\rangle$ を $|\tilde{k}\rangle$ が張る空間に直交する任意のベクトルとすると，すべての k に対して $\langle\psi|\tilde{k}\rangle\langle\tilde{k}|\psi\rangle = 0$，したがって

$$0 = \langle\psi|A|\psi\rangle = \sum_i \langle\psi|\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|\psi\rangle = \sum_i |\langle\psi|\tilde{\psi}_i\rangle|^2. \tag{2.173}$$

したがって，すべての i と $|\tilde{k}\rangle$ が張る空間に直交するすべての $|\psi\rangle$ に対して $\langle\psi|\tilde{\psi}_i\rangle = 0$ である．この結果，各々の $|\tilde{\psi}_i\rangle$ は $|\tilde{k}\rangle$ の線形結合 $|\tilde{\psi}_i\rangle = \sum_k c_{ik}|\tilde{k}\rangle$ で表される．$A = \sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_i |\tilde{\psi}_i\rangle\langle\tilde{\psi}_i|$ なので

$$\sum_k |\tilde{k}\rangle\langle\tilde{k}| = \sum_{kl}\left(\sum_i c_{ik}c_{il}^*\right)|\tilde{k}\rangle\langle\tilde{l}| \tag{2.174}$$

であることがわかる．オペレータ $|\tilde{k}\rangle\langle\tilde{l}|$ が線形独立であることが容易にわかるので，$\sum_i c_{ik}c_{il}^* = \delta_{kl}$ でなければならない．これにより c に余分の列を追加して，$|\tilde{\psi}_i\rangle = \sum_i v_{ik}|\tilde{k}\rangle$ なるユニタリー行列 v を作ることが保証される．ここで $|\tilde{k}\rangle$ のリストには 0 ベクトルを追加した．同様に $|\tilde{\varphi}_j\rangle = \sum_k w_{jk}|\tilde{k}\rangle$ なるユニタリー行列 w を見付けることができる．したがって，$|\tilde{\psi}_i\rangle = \sum_j u_{ij}|\tilde{\varphi}_j\rangle$ が得られる．ここで $u = vw^\dagger$ はユニタリーである． □

演習 2.72:（混合状態に対する Bloch 球） 純粋状態にある単一 q ビットに対する Bloch 球の描像は 1.2 節で紹介した．この記述は混合状態に対して次のように一般化される．

(1) 混合状態 q ビットの任意の密度行列は次のように書けることを示せ．

$$\rho = \frac{I + \vec{r}\cdot\vec{\sigma}}{2}, \tag{2.175}$$

ここで $\vec{r}$ は $\|\vec{r}\| \leq 1$ なる 3 次元実数ベクトルである．このベクトルを状態 ρ に対する **Bloch ベクトル** (Bloch vector) と呼ぶ．

(2) 状態 $\rho = I/2$ に対する Bloch ベクトル表現は何か？

(3) $\|\vec{r}\| = 1$ のときにのみ状態 ρ は純粋であることを示せ．

(4) 純粋状態に対してここで述べた Bloch ベクトルの記述は 1.2 節のものと一致することを示せ．

演習 2.73: ρ は密度オペレータであるとする．ρ に対する**極小アンサンブル**とは ρ の階数と同数の要素を持つアンサンブル $\{p_i, |\psi_i\rangle\}$ である．$|\psi\rangle$ は ρ の台における任意の状態とする．(Hermite オペレータ A の**台** (support) とは 0 でない A の固有ベクトルが張るベクトル空間である．) ρ に対して $|\psi\rangle$ を含む 最小アンサンブルが存在することを示せ．またそのアンサンブルで $|\psi\rangle$ が出現する確率は

$$p_i = \frac{1}{\langle\psi_i|\rho^{-1}|\psi_i\rangle} \tag{2.176}$$

であることを示せ．ここで ρ^{-1} は ρ が ρ の台にのみ作用するオペレータと考えられるときに，ρ の逆数として定義される．(この定義により ρ に逆数が存在しない場合を除外する．)

2.4.3　縮約した密度オペレータ

密度オペレータの最も奥深い応用は複合量子システムの**部分システム**を記述するツールであろう．その記述には**縮約した密度オペレータ** (簡約した—，reduced density operator) が用いられる．これが本項のテーマである．縮約した密度オペレータは非常に便利なので複合量子システムの解析には事実上不可欠である．

物理システム A と B があり，その状態は密度オペレータ ρ^{AB} で記述されるとする．システム A に対する縮約した密度オペレータは次式で定義される．

$$\rho^A \equiv \mathrm{tr}_B(\rho^{AB}). \tag{2.177}$$

ここで，tr_B はオペレータの写像でありシステム B に対する**部分トレース** (partial trace) と呼ぶ．部分トレースは

$$\mathrm{tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) \equiv |a_1\rangle\langle a_2| \ \mathrm{tr}(|b_1\rangle\langle b_2|) \tag{2.178}$$

で定義される．ここで $|a_1\rangle$, $|a_2\rangle$ は状態空間 A の任意の2つのベクトル，$|b_1\rangle$, $|b_2\rangle$ は状態空間 B の任意の 2 つのベクトルである．右辺のトレース演算はシステム B に対する通常のトレースであり，$\mathrm{tr}(|b_1\rangle\langle b_2|) = \langle b_2|b_1\rangle$ である．AB への演算の特別な部分クラスに対してのみ働く部分トレース演算を定義したが，式 (2.178) に加えて部分トレースが入力に対して線形であることを要請すると定義は完全になる．

コラム 2.6: なぜ部分トレースか？

なぜ部分トレースを使ってより大きな量子システムの 1 部分を記述できるのか？ この理由は部分トレース演算が，複合システムの部分システムに対する**観測可能** (observable) な量を正しく記述する，**一意** (unique) の演算であるからである．この意味を説明する．

M はシステム A の任意のオペレータであり， M を測定する測定器があるとする．複合システム AB に関して，同じ測定を行うときに対応する観測量を $\tilde{M}$ とする．$\tilde{M}$ は必然的に $M \otimes I_B$ に等しいことを示すのが差し当たっての目的である．M の固有状態が $|m\rangle$ で固有値が m, $|\psi\rangle$ が B の任意の状態とすると，もしシステム AB が状態 $|m\rangle|\psi\rangle$ にあるならば測定器は確率 1 で測定結果 m を与えなければならない．もし P_m が観測量 M の m 固有空間への射影オペレータとすると，これに対応する $\tilde{M}$ の射影オペレータは $P_m \otimes I_B$ である．したがって

$$\tilde{M} = \sum_m m P_m \otimes I_B = M \otimes I_B. \tag{2.179}$$

次のステップでは部分トレース手続きにより，システムの一部に対する観測の正しい統計が得られることを示す．システム A に対して観測量 M で記述される測定を行うとする．物理的矛盾を生じないために，システム A に「状態」ρ^A を関係づける処方箋は，ρ^A から計算しても ρ^{AB} から計算しても，測定結果の平均値が同じにならねばならない：

$$\mathrm{tr}(M\rho^A) = \mathrm{tr}(\tilde{M}\rho^{AB}) = \mathrm{tr}((M \otimes I_B)\rho^{AB}). \tag{2.180}$$

もし $\rho^A \equiv \mathrm{tr}_B(\rho^{AB})$ と 選べばこの式は確かに満たされる．実は部分トレー

スはこの性質を満たす**一意の関数**であることがわかる．一意性を確かめるために，すべての観測量 M に対して，$f(\cdot)$ は AB の密度オペレータから A の密度オペレータへの任意の写像であり次式を満たすとする：

$$\mathrm{tr}\big(Mf(\rho^{AB})\big) = \mathrm{tr}\big((M \otimes I_B)\rho^{AB}\big). \tag{2.181}$$

Hilbert-Schmidt の内積 $(X, Y) \equiv \mathrm{tr}(XY)$ に関する Hermite オペレータ空間に対するオペレータの正規直交基底を M_i とする（演習 2.39 と比較せよ）．この基底で $f(\rho^{AB})$ を展開すると

$$f(\rho^{AB}) = \sum_i M_i \mathrm{tr}\big(M_i f(\rho^{AB})\big) \tag{2.182}$$

$$= \sum_i M_i \mathrm{tr}\big((M_i \otimes I_B)\rho^{AB}\big). \tag{2.183}$$

この結果 f は式 (2.180) で一意に決定される．さらに部分トレースも式 (2.180) を満たすので，部分トレースはこの性質を持つ一意の関数である．

システム A の縮約した密度オペレータがどのような意味でもシステム A の状態を記述することは自明ではない．これが同一だと物理的に正当化するには，縮約した密度オペレータがシステム A に行う測定に対して，正しい統計を与えることを示さねばならない．これはコラム 2.6 で詳しく説明している．次の簡単な例題も縮約した密度オペレータを理解する助けになるであろう．まず量子システムが積状態 $\rho^{AB} = \rho \otimes \sigma$ にあるとする．ここで ρ はシステム A の密度オペレータ，σ はシステム B の密度オペレータとする．このとき

$$\rho^A = \mathrm{tr}_B(\rho \otimes \sigma) = \rho\ \mathrm{tr}(\sigma) = \rho, \tag{2.184}$$

これは我々が直観的に期待した結果である．同様に，この状態に対して $\rho^B = \sigma$ である．もっと重要な例は Bell の状態 $(|00\rangle + |11\rangle)/\sqrt{2}$ である．この密度オペレータは

$$\rho = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)\left(\frac{\langle 00| + \langle 11|}{\sqrt{2}}\right) \tag{2.185}$$

$$= \frac{|00\rangle\langle 00| + |11\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 11|}{2}. \tag{2.186}$$

第2のqビットについてトレースをとると，最初のqビットの縮約した密度オペレータが得られる．

$$\rho^1 = \mathrm{tr}_2(\rho) \tag{2.187}$$

$$= \frac{\mathrm{tr}_2(|00\rangle\langle 00|) + \mathrm{tr}_2(|11\rangle\langle 00|) + \mathrm{tr}_2(|00\rangle\langle 11|) + \mathrm{tr}_2(|11\rangle\langle 11|)}{2} \tag{2.188}$$

$$= \frac{|0\rangle\langle 0|\langle 0|0\rangle + |1\rangle\langle 0|\langle 0|1\rangle + |0\rangle\langle 1|\langle 1|0\rangle + |1\rangle\langle 1|\langle 1|1\rangle}{2} \tag{2.189}$$

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{2.190}$$

$$= \frac{I}{2}. \tag{2.191}$$

この状態は $\mathrm{tr}((I/2)^2) = 1/2 < 1$ であるから**混合状態**であることに注意する．これは注目すべき結果である．2つのqビットの結合システムは純粋状態，つまり**正確**に知ることができる．しかし第1のqビットは混合状態，つまり明らかに最大限の知識を持つことができない状態にある．システムの結合状態は完全に知ることができるが部分システムは混合状態にある，というこの奇妙な性質は量子もつれのもう1つのあかしである．

演習 2.74: A と B の複合システムが状態 $|a\rangle|b\rangle$ にあるとする．ここで $|a\rangle$ は A の純粋状態，$|b\rangle$ は B の純粋状態である．システム A のみの縮約した密度オペレータは純粋状態であることを示せ．

演習 2.75: 4つのBell状態の各々について，各qビットの縮約した密度オペレータを求めよ．

量子テレポーテーションと縮約した密度オペレータ

縮約した密度オペレータの有益な応用は量子テレポーテーションの解析である．1.3.7項より量子テレポーテーションは，AliceとBobがEPR対を共有し，かつ古典的な通信チャンネルがあるときに，AliceからBobへ量子情報を送る手続きであることを思い出そう．

一見したところテレポーテーションは光速より速い通信に使えそうに見えるが，相対性理論により堅く禁じられている．1.3.7 項において光速より速い通信を妨げるものは，Alice が測定結果を Bob に知らせる必要があることであると推測した．縮約した密度オペレータを使うとこれを厳密に示せる．

Alice が測定する直前の 3 つの q ビットの量子状態は（式 (1.32)）：

$$|\psi_2\rangle = \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big]. \tag{2.192}$$

Alice の計算基底で測定すると，測定後のシステムの状態は：

$$|00\rangle\Big[\alpha|0\rangle + \beta|1\rangle\Big],\quad 確率\ \frac{1}{4} \tag{2.193}$$

$$|01\rangle\Big[\alpha|1\rangle + \beta|0\rangle\Big],\quad 確率\ \frac{1}{4} \tag{2.194}$$

$$|10\rangle\Big[\alpha|0\rangle - \beta|1\rangle\Big],\quad 確率\ \frac{1}{4} \tag{2.195}$$

$$|11\rangle\Big[\alpha|1\rangle - \beta|0\rangle\Big],\quad 確率\ \frac{1}{4} \tag{2.196}$$

したがって，システムの密度オペレータは

$$\begin{aligned}\rho = \frac{1}{4}\Big[&|00\rangle\langle 00|(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|)\\ &+|01\rangle\langle 01|(\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|)\\ &+|10\rangle\langle 10|(\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|)\\ &+|11\rangle\langle 11|(\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)\Big]\end{aligned} \tag{2.197}$$

Alice のシステムのトレースをとると，Bob のシステムの縮約した密度オペレータは

$$\rho^B = \frac{1}{4}\Big[(\alpha|0\rangle + \beta|1\rangle)(\alpha^*\langle 0| + \beta^*\langle 1|) + (\alpha|1\rangle + \beta|0\rangle)(\alpha^*\langle 1| + \beta^*\langle 0|)$$
$$+(\alpha|0\rangle - \beta|1\rangle)(\alpha^*\langle 0| - \beta^*\langle 1|) + (\alpha|1\rangle - \beta|0\rangle)(\alpha^*\langle 1| - \beta^*\langle 0|)\Big] \tag{2.198}$$

$$= \frac{2(|\alpha|^2 + |\beta|^2)|0\rangle\langle 0| + 2(|\alpha|^2 + |\beta|^2)|1\rangle\langle 1|}{4} \tag{2.199}$$

$$= \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} \tag{2.200}$$

$$= \frac{I}{2}, \tag{2.201}$$

ここで最後の行で完全性関係を用いた．したがって，Alice が**測定を終了した後，** Bob が測定結果を**教わる前**の Bob の状態は $I/2$ である．この状態はテレポートされるべき状態 $|\psi\rangle$ と関係がなく，Bob が行う如何なる測定も $|\psi\rangle$ についての情報を含んでおらず，したがって Alice が Bob にテレポーテーションで光速よりも速く情報を送ることはできていない．

2.5 Schmidt 分解と純粋化

密度オペレータと部分トレースは，量子計算と量子情報の中心をなす複合量子システムの研究に有用な，並み居るツールの手始めにすぎない．高い価値があるツールをもう 2 つあげると **Schmidt 分解** (Schmidt decomposition) と**純粋化** (purification) である．本節ではこれら 2 つのツールとその実力の一端を紹介する．

定理 2.7:（Schmidt 分解） $|\psi\rangle$ は複合システム AB の純粋状態であるとする．次の関係を満たすシステム A の正規直交状態 $|i_A\rangle$ と，システム B の正規直交状態 $|i_B\rangle$ が存在する．

$$|\psi\rangle = \sum_i \lambda_i |i_A\rangle|i_B\rangle, \tag{2.202}$$

ここで λ_i は $\sum_i \lambda_i^2 = 1$ を満たす負でない実数であり，**Schmidt 係数** (Schmidt coefficient) と呼ぶ．

この結果は非常に便利である．その効力を見るために次の結論を考える：複合システム AB の純粋状態を $|\psi\rangle$ とする．Schmidt 分解により $\rho^A = \sum_i \lambda_i^2 |i_A\rangle\langle i_A|$

および $\rho^B = \sum_i \lambda_i^2 |i_B\rangle\langle i_B|$，したがって ρ^A と ρ^B の固有値は同一，つまり両オペレータに対して λ_i^2 である．量子システムの多くの重要な性質がシステムの縮約した密度オペレータの固有値で完全に決定されるので，複合システムの純粋状態に対してそのような性質は2つのシステムで同じになる．例えば2個のqビット状態 $(|00\rangle + |01\rangle + |11\rangle)/\sqrt{3}$ を考える．これには明らかな対称性はないが，$\mathrm{tr}((\rho^A)^2)$ と $\mathrm{tr}((\rho^B)^2)$ を計算するとそれぞれ 7/9 の同じ値を持つことがわかる．これは Schmidt 分解のほんのちょっとした結果にすぎない．

証明　システム A と B が同次元の状態空間を持つ場合について証明し，一般の場合は演習 2.76 に残す．$|j\rangle$ と $|k\rangle$ はシステム A, B に対する任意の固定した正規直交基底であるとする．このとき複素数 a_{jk} のある行列 a に対して，$|\psi\rangle$ は次のように書ける．

$$|\psi\rangle = \sum_{jk} a_{jk}|j\rangle|k\rangle. \tag{2.203}$$

特異値分解により $a = udv$，ここで d が負でない要素を持つ対角行列，u と v をユニタリー行列である．したがって

$$|\psi\rangle = \sum_{ijk} u_{ji}d_{ii}v_{ik}|j\rangle|k\rangle. \tag{2.204}$$

$|i_A\rangle \equiv \sum_j u_{ji}|j\rangle$，$|i_B\rangle \equiv \sum_k v_{ik}|k\rangle$ および $\lambda_i \equiv d_{ii}$ と定義すると，

$$|\psi\rangle = \sum_i \lambda_i|i_A\rangle|i_B\rangle. \tag{2.205}$$

u がユニタリーで $|j\rangle$ が正規直交であることから，$|i_A\rangle$ が正規直交集合を形成すること，および $|i_B\rangle$ も同様であることが容易にわかる．　□

演習 2.76: A と B の状態空間が異なる次元を有する場合に Schmidt 分解を拡張せよ．

演習 2.77: ABC が3成分の複合システムであるとする．そのようなシステムには

$$|\psi\rangle = \sum_i \lambda_i|i_A\rangle|i_B\rangle|i_C\rangle \tag{2.206}$$

の形に書けない量子状態 $|\psi\rangle$ が存在することを例をあげて示せ．ここで λ_i は実数，$|i_A\rangle$，$|i_B\rangle$，$|i_C\rangle$ は各システムの正規直交基底である．

基底 $|i_A\rangle$，$|i_B\rangle$ をそれぞれ A，B に対する **Schmidt 基底** (Schmidt basis)，0 でない値を持つ λ_i の数を状態 $|\psi\rangle$ に対する **Schmidt 数** (Schmidt number) と呼ぶ．Schmidt 数は複合量子システムの重要な性質であり，ある意味でシステム A とシステム B の間のもつれの「量」に相当する．なぜこうなのかを示すために，明らかではあるが重要な次の性質を考える．Schmidt 数はシステム A もしくはシステム B のみに働くユニタリー変換のもとで保存される．これを検証するために，もし $\sum_i \lambda_i|i_A\rangle|i_B\rangle$ が $|\psi\rangle$ の Schmidt 分解ならば，$\sum_i \lambda_i(U|i_A\rangle)|i_B\rangle$ は $U|\psi\rangle$ に対する Schmidt 分解である．ここで U はシステム A のみに働くユニタリーオペレータである．この形の幾何学的不変性があるので Schmidt 数は非常に便利なツールになる．

演習 2.78: 複合システム AB の状態 $|\psi\rangle$ は Schmidt 数が 1 のときにのみ積状態になることを証明せよ．ρ^A（したがって ρ^B）が純粋状態であるときにのみ $|\psi\rangle$ は積状態になることを証明せよ．

量子計算と量子情報に関連する 2 番目のテクニックは**純粋化**(purification) である．量子システム A の状態 ρ^A が与えられるとする．もう 1 つのシステム R を導入し，複合システム AR に対して，$|AR\rangle$ なる**純粋状態を定義**して $\rho^A = \mathrm{tr}_R(|AR\rangle\langle AR|)$ を満たすようにすることができる．つまりシステム A のみを見た場合に，純粋状態 $|AR\rangle$ は ρ^A に縮約される．これは**純粋化**と呼ぶ純粋に数学的手続きであり，これを用いて純粋状態を混合状態に関連付けることができる．この理由でシステム R を**参照システム** (reference system) と呼ぶ．これは仮想的システムであり直接の物理的意味はない．

任意の状態に対して純粋化ができるのを証明するために，ρ^A に対するシステム R と純粋状態 $|AR\rangle$ を如何にして作るかを説明する．ρ^A は正規直交分解 $\rho^A = \sum_i p_i|i^A\rangle\langle i^A|$ を持つとする．ρ^A を純粋化するために A と同じ状態空間を持ち正規直交基底 $|i^R\rangle$ を持つシステム R を導入し，複合システムに対する純粋状態を次のように定義する．

$$|AR\rangle \equiv \sum_i \sqrt{p_i}|i^A\rangle|i^R\rangle. \tag{2.207}$$

次に状態 $|AR\rangle$ に対応するシステム A の縮約した密度オペレータを計算する．

$$\mathrm{tr}_R(|AR\rangle\langle AR|) = \sum_{ij} \sqrt{p_i p_j}|i^A\rangle\langle j^A|\ \mathrm{tr}(|i^R\rangle\langle j^R|) \tag{2.208}$$

$$= \sum_{ij} \sqrt{p_i p_j}|i^A\rangle\langle j^A|\delta_{ij} \tag{2.209}$$

$$= \sum_{i} p_i|i^A\rangle\langle i^A| \tag{2.210}$$

$$= \rho^A. \tag{2.211}$$

したがって，$|AR\rangle$ は ρ^A の純粋化である．

Schmidt 分解と純粋化の間の深い関係について注意しておく．システム A の混合状態を純粋化する手続きとは，次のように純粋状態を定義することである．つまりその純粋状態のシステム A に対する Schmidt 基底は混合状態を対角化する基底とし，Schmidt 係数は純粋化するべき密度オペレータの固有値の平方根とする．

本節では複合量子システムを研究するための 2 つのツール，つまり Schmidt 分解と純粋化について説明した．これらのツールは量子計算と量子情報，特に本書第 3 部の主題である量子情報の研究に不可欠のものである．

演習 2.79: 2 個の q ビットよりなる複合システムを考える．次の状態の Schmidt 分解を求めよ．

$$\frac{|00\rangle+|11\rangle}{\sqrt{2}};\ \frac{|00\rangle+|01\rangle+|10\rangle+|11\rangle}{2};\ \frac{|00\rangle+|01\rangle+|10\rangle}{\sqrt{3}}. \tag{2.212}$$

演習 2.80: 2 つのシステム成分 A, B より成る複合量子システムの 2 つの純粋状態を $|\psi\rangle, |\varphi\rangle$ とし，Schmidt 係数は同一であるとする．$|\psi\rangle = (U \otimes V)|\varphi\rangle$ を満たすシステム A のユニタリー変換 U と，システム B のユニタリー変換 V が存在することを示せ．

演習 2.81:（純粋化の自由度）　複合システム AR に対する状態 ρ^A の 2 つの純粋化を $|AR_1\rangle$ と $|AR_2\rangle$ とする．システム R に働き $|AR_1\rangle = (I_A \otimes U_R)|AR_2\rangle$ を満たすユニタリー変換 U_R が存在することを証明せよ．

演習 2.82: $\{p_i, |\psi_i\rangle\}$ は量子システム A に対する密度行列 $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$ を生成する状態のアンサンブルであるとする．正規直交基底 $|i\rangle$ を持つシステム R を導入する．

(1) $\sum_i \sqrt{p_i}|\psi_i\rangle|i\rangle$ は ρ の純粋化であることを示せ.

(2) 基底 $|i\rangle$ で R を測定して結果 i を得たとする. 結果 i を得る確率はいくらか, また対応するシステム A の状態は何か？

(3) $|AR\rangle$ はシステム AR に対する ρ の**任意の**純粋化であるとする. R を測定するとシステム A の測定後の状態が $|\psi_i\rangle$, 確率が p_i になる正規直交基底 $|i\rangle$ が存在することを示せ.

2.6 EPR と Bell の不等式

量子力学に衝撃を受けなかった人は理解していなかった人であった.
— Niels Bohr

散歩の途中で Einstein が突然立ち止まり私のほうを向いて, 月を見るときに月が存在していると本当に信じるかと私に聞いた. その後散歩の間中「存在する」という言葉で物理学者が何を意味するべきかを議論した. — Abraham Pais

... 量子現象は Hilbert 空間で起きるのではない. それは実験室で起きるものである. — Asher Peres

... 不可能性の証明で証明されるものは想像力の欠如である.
— John Bell

本章では量子力学のツールと数学の紹介に焦点を絞ってきた. 次章以降でこれらのテクニックを応用するに際して繰り返し登場するテーマは, 量子力学の普通でない**非古典的**性質である. しかし正確なところ量子力学と古典的世界との違いは何であろうか？ この違いを理解することが, 古典物理学では困難ないし不可能な情報処理タスクを, 如何に行うかを知る死命を制することになる. 本章を締めくくるに当たり, この節では量子力学と古典物理学の本質的相違を納得させずには置かない Bell の不等式を議論する.

我々は人や本のような対象物の話をするとき，その対象物は観測とは無関係に存在すると仮定している．つまり測定はそのような物理的性質を**現す**ためだけに働く．例えばテニスのボールは**位置**という物理的性質を持っており，通常我々はそれをボール表面で反射した光で測定する．1920 年代から 30 年代にかけて量子力学が育つにつれて，古典的見方とは著しく異なった奇妙な見方が現れてきた．本章の始めに述べたように量子力学によれば，観測しない粒子は，観測と無関係に存在する物理的性質を持っていない．むしろそのような物理的性質はシステムを観測した結果として生まれる．例えば量子力学によれば，q ビットは「z 方向のスピン σ_z」や「x 方向のスピン σ_x」という決まった性質は持っておらず，それらを適切に測定することによって現れる．むしろ量子力学は状態ベクトルが与えられて観測量 σ_z が測定されたとき，あるいは観測量 σ_x が測定されたときに，可能な測定結果の確率を規定する一連のルールを与える．

多くの物理学者は自然界へのこの新たな見方を拒絶した．最も卓越した反対者は Albert Einstein であった．Boris Podolsky，Nathan Rosen と共著の有名な「EPR 論文」で Einstein は思考実験を提案し，「量子力学は自然界を完全に記述しない」と彼が信じるところを示した．

EPR の議論の本質は次の通りである．EPR は彼らが「実在の要素」(elements of reality) と名付けたものに興味を持った．彼らの信じたところは，如何なる実在の要素も完全な物理学理論で表現され**なければならない**．議論のゴールは量子力学に含まれていない実在の要素を指摘することによって，量子力学が完全な物理学理論でないと示すことにあった．これを試みた彼らの方法は，物理的性質に対する**十分条件**と主張するものを実在の要素として導入すること，つまり測定直前にその性質が持つ値を確実に予想できるようにすることであった．

コラム 2.7: EPR 実験における反相関

歴史的理由で**スピン 1 重項** (spin singlet) と呼ばれる 2 つの q ビット状態

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}, \tag{2.213}$$

を用意する．この状態が 2 つの q ビットシステムのもつれ状態であることを示すのは難しくない．両方の q ビットで $\vec{v}$ 軸方向のスピンを測定するとする．つまり（式 (2.116) で定義された）観測量 $\vec{v}\cdot\vec{\sigma}$ を測定し，各 q ビットについて結果 $+1$ または -1 を得る．$\vec{v}$ をどう選択するかにかかわりなく 2 つの測定結果は常に互いに異なる．つまり，もし最初の q ビットの測定で $+1$ が得られれば，第 2 の q ビットの測定で -1 が得られ，あるいはその逆になる．それはあたかも第 2 の q ビットが，最初の測定がどう行われたかと無関係に，結果を知っているかのようである．なぜこうなるかを見るために，$|a\rangle$ と $|b\rangle$ が $\vec{v}\cdot\vec{\sigma}$ の固有状態であるとする．このとき

$$|0\rangle = \alpha|a\rangle + \beta|b\rangle \tag{2.214}$$

$$|1\rangle = \gamma|a\rangle + \delta|b\rangle \tag{2.215}$$

を満たす複素数 $\alpha, \beta, \gamma, \delta$ が存在する．代入すると，

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = (\alpha\delta - \beta\gamma)\frac{|ab\rangle - |ba\rangle}{\sqrt{2}}. \tag{2.216}$$

しかし $\alpha\delta - \beta\gamma$ はユニタリー行列 $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ の行列式であり，ある実数 θ に対して位相因子 $e^{i\theta}$ に等しい．したがって，観測されないグローバル位相因子を除いて

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}} = \frac{|ab\rangle - |ba\rangle}{\sqrt{2}}. \tag{2.217}$$

その結果，両方の q ビットに対して $\vec{v}\cdot\vec{\sigma}$ を測定すると，最初の q ビットに対する $+1$ (または -1) が第 2 の q ビットに対する -1 (または $+1$) を意味する．

例えばqビットのもつれ対をそれぞれAliceとBobが持っていると考える.

$$\frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.218}$$

AliceとBobは互いに遠く隔たっているとする. Aliceは$\vec{v}$軸方向のスピン測定, つまり（式(2.116)で定義された）観測量$\vec{v}\cdot\vec{\sigma}$の測定を行う. Aliceは測定結果+1を得たとする. すると（コラム2.7に示した）簡単な量子力学の計算により, Bobも$\vec{v}$軸に沿って彼のqビットをスピンを測定すると, 結果−1を得ることを彼女は誤りなく予想できる. 同様にAliceが−1と測定すると, Bobのqビットの測定結果が+1であることを確実に予想できる. 何時もAliceがBobのqビットに対する$\vec{v}$方向の測定結果を予測できるので, その物理的性質はEPRの基準によれば実在の要素であり, 完全な物理学理論によって表されなければならない. しかし標準的量子力学は我々が示したように, もし$\vec{v}\cdot\vec{\sigma}$を測定したときの各々の測定結果の確率をどう計算すればよいかを示すにすぎない. 確かに標準的量子力学はすべての単位ベクトル$\vec{v}$に対して, $\vec{v}\cdot\vec{\sigma}$の値を示すように意図された基本的要素を何も含んでいない.

量子力学が彼らの基準でいう何か本質的な「実在の要素」を欠いているのを示すことで, 量子力学が不完全なことを示すのがEPRのゴールであった. 彼らはなされた測定と無関係に存在する性質をシステムが備えているような, 古典的自然観に返すことを望んでいた. EPRにとって不幸なことに, 多くの物理学者はこの推論に納得せず受け入れなかった. 絶対命令によって従うべき性質を自然界に課そうとする試みは, 自然界の法則を研究する方法として奇妙なものに見える.

実際自然界は最後にEPRに勝った. EPR論文の発表後30年近く経ってから, EPRが押し返そうとした自然描像の正否を検証するのに用いることができるような**実験によるテスト**が提案された. この結果自然はこの見解を**実験的に無効**にして, 量子力学に同意を与えたのである.

この実験的無効の鍵は**Bellの不等式** (Bell's inequality) として知られている成果である. Bellの不等式は量子力学に関する結果ではないので, しばらく量子力学のことは**忘れる**ことにする. Bellの不等式を得るには思考実験を行う. これは自然界が従うべきとEinsteinと協力者が考えたように, 自然の働きについての考えを我々の常識で解析することである. 常識で解析した後で量子力学的解析を

行い**常識の解析と一致しない**ことを示す．次に実際の実験を通じて，自然の働きに関する我々の常識か量子力学かを自然界に決めてもらう．

図 2.4 に示すような次の実験を想定する．Charlie は 2 つの粒子を用意する．彼がどのように粒子を用意するかは問わないこととし，ただ彼が実験を繰り返し実行できるとする．一度用意すると彼は 1 つの粒子を Alice に他の 1 つを Bob に送る．

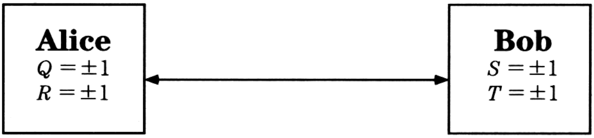


図 2.4: Bell の不等式に対する実験構成の模式図．Alice は Q か R のいずれを測定するか選ぶことができ Bob は S か T を選べる．彼らは測定を同時に行う．Alice と Bob は十分遠く離れており一方のシステムの測定が他方に影響することはない．

Alice が粒子を受け取ると彼女はそれを測定する．彼女は 2 つの測定装置を使うことができ 2 つの異なる測定のうちの一方を選択できる．この測定は物理的性質 — P_Q と P_R と呼ぶ — に関するものである．Alice はあらかじめどちらの測定をするか決めておらず，粒子を受け取ってからコインを投げるか何かランダムな方法で，どちらの実験を行うかを決める．簡単のためにいずれの測定も結果は $+1$ か -1 か，2 つのうちの 1 つであるとする．仮に Alice の粒子が性質 P_Q に対して値 Q を持つとする．Q は Alice の粒子の**対象物の性質**であるとし，ちょうどテニスのボールの位置がそれから散乱される光で現されると想像するように，測定によってはじめて現れる．同様に R は性質 P_R を測定することによって現れる．

同様に Bob は 2 つの性質 P_S または P_T を測定することができ，これらの性質に対して対象が有している値 S または T — 各々 $+1$ か -1 かの値をとる — を現す．Bob はあらかじめどちらの性質を測定するか決めておらず，粒子を受け取ってからランダムに決める．実験のタイミングは Alice と Bob が**同時に**（あるいは相対論の正確な言葉を使えば因果律で結合していない方法で）行う．したがって，物理的影響は光速より速く伝わらないので，Alice が行う測定が Bob の測定を乱すことはない（また逆も同じ）．

$QS + RS + RT - QT$ なる量に関して簡単な代数計算を行う．

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T \tag{2.219}$$

において R, $Q = \pm 1$ なので $(Q + R)S = 0$ または $(R - Q)T = 0$ のいずれかが成り立つ．(2.219) よりいずれの場合にも $QS + RS + RT - QT = \pm 2$ である．次に $p(q, r, s, t)$ は測定前にシステムが $Q = q$, $R = r$, $S = s$, $T = t$ の値をとる確率であるとする．これらの確率は Charlie の準備の仕方と雑音に依存するかも知れない．$\mathbf{E}(\cdot)$ が平均値を表すとすると，

$$\mathbf{E}(QS + RS + RT - QT) = \sum_{qrst} p(q, r, s, t)(qs + rs + rt - qt) \tag{2.220}$$

$$\leq \sum_{qrst} p(q, r, s, t) \times 2 \tag{2.221}$$

$$= 2. \tag{2.222}$$

また

$$\mathbf{E}(QS + RS + RT - QT) = \sum_{qrst} p(q, r, s, t)qs + \sum_{qrst} p(q, r, s, t)rs$$

$$+ \sum_{qrst} p(q, r, s, t)rt - \sum_{qrst} p(q, r, s, t)qt \tag{2.223}$$

$$= \mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT). \tag{2.224}$$

式 (2.222) と (2.224) を比べると **Bell の不等式**を得る．

$$\mathbf{E}(QS) + \mathbf{E}(RS) + \mathbf{E}(RT) - \mathbf{E}(QT) \leq 2. \tag{2.225}$$

この結果は 4 人の発見者の頭文字をとって **CHSH 不等式**とも呼ぶ．これは Bell が最初に見付けて以来，Bell の不等式と総称する不等式群の一部である．

実験を何度も繰り返すことにより，Alice と Bob は Bell の不等式の左辺の量を決めることができる．例えば，一連の実験を繰り返した後で，Alice と Bob が一ヶ所に集まってデータを解析する．Alice が P_Q を測定し Bob が P_S を測定したすべての実験を見て，実験結果を掛け合わせ QS の値のサンプルを得る．このサンプルの平均値をとると，行った実験の回数だけで決まる精度で $\mathbf{E}(QS)$ を推

定できる．同様に Bell の不等式の左辺にある他の量もすべて推定すると，実際の実験で不等式が成立するかどうかがわかる．

この描像に量子力学を持ち込もう．次のような量子力学の実験を行うとする．Charlie は次の状態にある 2 個の q ビットを準備する．

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}. \tag{2.226}$$

彼は最初の q ビットを Alice に渡し，第 2 の q ビットを Bob に渡す．彼らは次の観測量の測定を行う．

$$Q = Z_1, \quad S = \frac{-Z_2 - X_2}{\sqrt{2}}, \tag{2.227}$$

$$R = X_1, \quad T = \frac{Z_2 - X_2}{\sqrt{2}}. \tag{2.228}$$

簡単な計算によりこれら観測量に対する平均値を量子力学の記号 $\langle \cdot \rangle$ で書くと

$$\langle QS \rangle = \frac{1}{\sqrt{2}}; \ \langle RS \rangle = \frac{1}{\sqrt{2}}; \ \langle RT \rangle = \frac{1}{\sqrt{2}}; \ \langle QT \rangle = -\frac{1}{\sqrt{2}}, \tag{2.229}$$

したがって

$$\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2}. \tag{2.230}$$

ちょっと待って欲しい！ 我々は式 (2.225) で QS の平均値と RS の平均値と RT の平均値を加え QT の平均値を引くと，決して 2 を越えないことを知った．にもかかわらずここでは量子力学はこれら平均値の和が $2\sqrt{2}$ になっている！

幸いにして我々は自然界にこの明白なパラドックスを解いてもらうように求めることができる．光子 — 光の粒子 — を用いて，量子力学の予想 (2.230) と我々の常識的推論より導いた Bell の不等式 (2.225) を検証する巧妙な実験が行われた．実験の詳細は本書の範囲外であるが，結果は目覚ましくも量子力学の予想に有利なものであった．自然は Bell の不等式 (2.225) には従わない．

これは何を意味するのか？ Bell の不等式を導く際に入った，仮定が正しくなかったに違いない．この種の議論をなしえる種々な形式を解析し，Bell 類似の不等式を導く微妙に異なる仮定を解析した膨大な論文が執筆された．ここでは主要点のみをまとめる．

式 (2.225) の証明において疑わしい仮定が 2 つある：

(1) 物理的性質 P_Q，P_R，P_S，P_T が，観測とは独立に存在する確定した値 Q，R，S，T を持つという仮定．これは**実在性** (realism) の仮定と呼ばれる．

(2) Alice が行う測定が Bob の測定に影響しないという仮定．これは**局在性** (locality) の仮定と呼ばれる．

これら 2 つの仮定を合わせて**局在的実在性** (local realism) の仮定と呼ばれる．これらは確かに自然の動きに関して直観的にもっともな仮定であり，日常の経験に合致している．にもかかわらず Bell の不等式は，これら仮定の少なくとも 1 つは正しくないことを示している．

Bell の不等式から学ぶべきものは何か？ 物理学者にとって最も重要な教えは，自然の動きに関して彼らが根強く持っている常識的直観が間違っていることである．自然は局在的に実在いていない．たいていの物理学者は，量子力学において我々の自然像から省かねばならないものは実在性の仮定である，という見解を持っており，他の物理学者はその代わりに局在性の仮定を省くべきだと議論してきた．それにもかかわらず今では Bell の不等式と重要な実験的証拠が示すところによれば，もし我々が量子力学を直観的によく理解しようとするならば，我々の自然観から局在性と実在性のいずれか一方，または両方を取り除かねばならない．

量子計算と量子情報の分野は Bell の不等式から何を学ぶべきか？ 歴史的に最も有益な教えもまた漠然としたものであった： EPR 状態のようなもつれ状態に関して何か奥深い「前向き」のものがある．量子計算と特に量子情報において，簡単な質問をすることによって多くの得るものがあった：「この問題においてもつれは何をもたらすか？」テレポーテーションや超高密度符号化で見たようにまた本書でこれから繰り返し見るように，もつれを問題と結びつけることによって古典情報では想像できなかった新しい可能性の世界を開くことができる．より大きな未来を描けば，もつれが基本的に自然の新しいリソースであり，本質的に古典的リソースを**越える**ものであることを Bell の不等式は教えている．丁度古い青銅器時代に対する鉄器時代の到来のように．量子計算と量子情報の主要な役割はこの新しいリソースを利用して，古典的リソースでは難しかったあるいは不可能であった情報処理を行うことである．

問題 2.1:（Pauli の行列の機能） $f(\cdot)$ は複素数から複素数への任意の関数とする．$\vec{n}$ は 3 次元の正規化ベクトル，θ は実数とする．次式が成立すること

を示せ.

$$f(\theta\vec{n}\cdot\vec{\sigma}) = \frac{f(\theta)+f(-\theta)}{2}I + \frac{f(\theta)-f(-\theta)}{2}\vec{n}\cdot\vec{\sigma}. \tag{2.231}$$

問題 2.2:（Schmidt 数の性質） $|\psi\rangle$ は構成システム A, B よりなる複合システムの純粋状態とする.

(1) $|\psi\rangle$ の Schmidt 数は縮約した密度行列 $\rho_A \equiv \mathrm{tr}_B(|\psi\rangle\langle\psi|)$ の階数に等しいことを示せ.（Hermite オペレータの階数 (rank) はその台 (support) の次元に等しい.）

(2) $|\alpha_j\rangle$ と $|\beta_j\rangle$ がそれぞれシステム A と B の（正規化されていない）状態であるとき，$|\psi\rangle = \sum_j |\alpha_j\rangle|\beta_j\rangle$ は $|\psi\rangle$ に対する表現であるとする. この分解の項数は $|\psi\rangle$ の Schmidt 数 $\mathrm{Sch}(\psi)$ より大きいか等しいことを証明せよ.

(3) $|\psi\rangle = \alpha|\varphi\rangle + \beta|\gamma\rangle$ とする. 次式を証明せよ.

$$\mathrm{Sch}(\psi) \geq |\mathrm{Sch}(\varphi) - \mathrm{Sch}(\gamma)|. \tag{2.232}$$

問題 2.3:（Tsirelson の不等式） 実数の単位ベクトル $\vec{q}$, $\vec{r}$, $\vec{s}$, $\vec{t}$ に対して $Q = \vec{q}\cdot\vec{\sigma}$, $R = \vec{r}\cdot\vec{\sigma}$, $S = \vec{s}\cdot\vec{\sigma}$, $T = \vec{t}\cdot\vec{\sigma}$ とする.

$$(Q\otimes S + R\otimes S + R\otimes T - Q\otimes T)^2 = 4I + [Q,R]\otimes[S,T]. \tag{2.233}$$

を示せ. この結果を用いて

$$\langle Q\otimes S\rangle + \langle R\otimes S\rangle + \langle R\otimes T\rangle - \langle Q\otimes T\rangle \leq 2\sqrt{2} \tag{2.234}$$

であり，式 (2.230) で見出した Bell の不等式の破れは，量子力学において最大限可能であることを証明せよ.

歴史と参考資料

高等学校から大学院レベルに至る線形代数に関して多くの書物がある．多分我々が気に入っているのは Horn と Johnson による 2 巻 [HJ85] [HJ91] であり，広範囲の内容をわかりやすくカバーしている．その他の有益な資料には Marcus と Minc [MN92]，Bhatia [Bha97] がある．線形代数の良い入門書には Halmos [Hal58]，Perlis [Per52]，Strang [Str76] がある．

量子力学について多くの優れた書物がある．不幸にしてこれらの多くは量子計算と量子情報からは逸脱した話題に焦点を当てている．多分，今ある最も関連の深い書物は Peres の素晴らしい本 [Per93] である．Peres は初歩的量子力学を非常に明快に提示しただけでなく Bell の不等式や関連した結果を広く議論している．入門レベルの良書には Sakurai の本 [Sak95]，Feynman, Leighton, Sands の優れたシリーズの第 3 巻　[FLS65a]，Cohen-Tannoudji, Diu, Laloë の 2 巻の本 [CTDL77a] [CTDL77b] がある．これら 3 種の書物のそれぞれの内容は大部分が依然として量子計算と量子情報から離れた応用を扱っているが，他の多くの量子力学のテキストより量子計算と量子情報の精神に近い．その結果量子計算と量子情報を学ぶ興味を持っている読者はこれらを詳しく読む必要はない．しかしこれらのどれか 1 つがあれば，特に物理学者の論文を読むときに参考書として役立つ．量子力学の歴史に関する参考文献は 1 章の最後に掲げた．

多くの量子力学の教科書では射影オペレータしか扱っていない．量子計算と量子情報への応用では，射影オペレータを特別ケースとして扱う測定の一般論から出発するのが有益である．またこれが初心者にも容易であると信じる．もちろん究極的にはすでに示したように 2 つのアプローチは等価である．ここで採用した一般測定理論は 1940 年代から 1970 年代にかけて進展した．この歴史は Kraus の本 [Kra83] から読みとれる．量子測定に関する興味ある議論が Gardiner [Gar91] の 2.2 節と Braginsky, Khahili の本 [BK92] に見られる．2.2.6 節で述べた異なる非直交状態に対する POVM 測定は Peres [Per88] による．演習 2.64 で述べた拡張は Duan, Guo [DG98] に出ている．

超高密度符号化は Bennett, Wiesner [BW92] により発明された．もつれ状態を使った変形した超高密度符号化の実験は Mattle, Weinfurter, Kwiat, Zeilinger [MWKZ96] により行われた．

密度オペレータ形式は Landau [Lan27] と von Neumann [von27] により独立に導入された．密度行列に対するアンサンブルの自由度(定理 2.6)は最初 Schrödinger [Sch36] が指摘しその後 Jaynes [Jay57]，Hughston, Jozsa, Wootters [HJW93] により再発見された．演習 2.73 の結果は Jaynes の論文に拠っており演習 2.81, 2.82 は Hughston, Jozsa, Wootters の論文に出ている．与えられた密度行列に対する密度行列分解に出てくる確率分布のクラスは Uhlmann [Uhl70] と Nielsen [Nie99b] により研究された．Schmidt の名を取った分解は [Sch06] に発表された．演習 2.77 の結果は Peres [Per95] に出てくる．

EPR 思考実験は Einstein, Podolsky, Rosen [EPR35] によっており，ここで示した形に書き直したのは Bohm [Boh51] である．これはときどき誤って EPR「パラドックス」と引用される．Bell の不等式はこの形の不等式を最初に導いた Bell [Bel64] に敬意を表して名付けられた．ここで示した形は Clauser, Horne, Shimony, Holt [CHSH69] により提出され，CHSH 不等式と呼ぶ．この不等式は Bell によって独立に導かれたが発表されなかった．

問題 2.2 の(3)は Thapliyal(私信)による．Tsirelson の不等式は Tsirelson[Tsi80] による．

第3章　コンピュータ科学入門

自然科学では自然が我々に世界を与えてくれて，我々がその法則を発見するだけである．コンピュータではそれに法則を吹き込み，世界を創造する．— Alan Kay

我々の分野はまだ萌芽期にある．2000 年にわたる経験を積んでいないのは素晴らしいことである．我々の目前で非常に重要な結果が現れる段階にいるのである．
— Michael Rabin，コンピュータ科学について．

アルゴリズム (algorithm) はコンピュータ科学の鍵となる概念である．アルゴリズムは子供のときに学んだ 2 つの数を足すといった，あるタスクを実行するための正確な処方箋である．本章ではコンピュータ科学により発展した近代的アルゴリズム理論について概説する．アルゴリズムの基本モデルは **Turing 機械** (Turing machine) である．これは現代のパーソナルコンピュータに似ている理想化されたコンピュータであり，より簡単な基本仕様と理想化された無制限のメモリを持っている．この Turing 機械は見かけ上簡単なので誤解されやすいが，実は非常に強力なデバイスなのである．これによっておよそあらゆるアルゴリズムを — 明らかにより強力なコンピュータで働くアルゴリズムでも — 実行できる．

アルゴリズムを学ぶに当たって明らかにしたい基本的疑問は，与えられたタスクを行うに必要なリソースは何か？である．この疑問は 2 つにわかれる．第 1 はできれば特定の問題を解くための具体的アルゴリズムを示したうえで，どのような計算タスクが可能かを理解したい．例えば，我々は数字のリストを小さい順に手早く並べ替える優れたアルゴリズムを多数持っている．疑問の第 2 の側面は達

成できる計算タスクの**限界** (limitation) を示すことである．例えば，数字のリストを小さい順に並べ替えるアルゴリズムによって行う演算回数の下界を与えることができる．これら2つのタスク — 計算問題を解くアルゴリズムと計算問題を解く能力の限界を示すアルゴリズム— が緊密につながるのが理想である．現実には計算問題を解くために知られている最良の技術と，解法に関して知られている最も厳密な限界の間にはかなりのギャップが存在することが多い．本章の目的は計算問題の解析とそのような問題を解くアルゴリズムの作成・解析をサポートするために開発されたツールを幅広く概観することにある．

なぜ**量子計算** (quantum computation) と**量子情報** (quantum information) に興味を持つ人が**古典**コンピュータ科学を調べることに時間を使うのか？ この努力をするには理由が3つある．第1の理由は古典コンピュータ科学において広い概念と技術体系ができており，これを量子計算と量子情報の努力に再利用し得ることである．量子計算と量子情報における多くの成功例は，コンピュータ科学の既存の概念と，量子力学の新しい概念とを組み合わせることにより生まれた．例えば量子コンピュータの幾つかの高速アルゴリズムは，古典アルゴリズムでよく使われた強力なツールである Fourier 変換に根ざしている．ひとたび量子コンピュータが Fourier 変換を古典コンピュータより高速で実行できることが理解されると，多くの重要な量子アルゴリズムが開発されるようになる．

第2にコンピュータ科学者は，古典コンピュータ上で与えられた計算タスクを行うに必要なリソースを理解するために，多大の努力を重ねてきた．この結果が量子計算や量子情報と比較する根拠としても使えるのである．例えば与えられた数の素因数を見出す問題に関心が集まった．古典コンピュータではこの問題は「効率的な」解を持たないと信じられている —「効率的」の意味は本章で後で説明する．わかったことは素因数を見出す問題において，古典コンピュータでできることと量子コンピュータでできることの間には，ギャップがあることである．これ自身が興味深いと同時に，もっと広い意味でそのようなギャップが単に素因数分解に限らず，もっと広いクラスの計算問題にも存在するかも知れないと示唆している点で興味深い．この特定の問題をさらに研究することにより，どのような問題が古典コンピュータ上より，量子コンピュータ上のほうが扱いやすいかがわかるかも知れない．そのうえでこの洞察に基づいて，他の問題に対する興味深い量子アルゴリズムの発見を目指すことができる．

3番目のそして最も重要な理由は，コンピュータ科学者の**思考**を学ぶことができることである．コンピュータ科学者は物理学者や他の自然科学者と少し異なる考え方をする．量子計算と量子情報を深く理解しようとする人は少なくともある時間はコンピュータ科学者のように考えることを学ばねばならない．どんな問題があるか，より重要なのはコンピュータ科学者が最も興味を持っている問題は何か，ということを直観的に知っていなければならない．

本章の構成は次のようになっている．3.1節で計算の2つのモデル，つまりTuring機械モデルと回路モデルを紹介する．我々の計算の基本モデルおしてTuring機械モデルを使用する．しかし具体的な場合にはほとんど計算の回路モデルを使用し，これが量子計算の研究に最も有用となる．計算モデルを手に入れたところで，残りの節では計算に必要なリソースを議論する．3.2節で始めに我々が興味の対象とする計算タスクを概観して，関連するリソースの疑問を議論する．次に**計算量** (computational complexity) の主要概念を広く見渡す．この分野では特定の問題を解くに要する時間と空間の要請を調べ，解の困難さに則って広く問題を分類する．この節の最後に計算を行うに要するエネルギーリソースを調べる．驚くことにもし計算を可逆にできれば，計算を実行するに要するエネルギーは無視できるほど小さいことがわかる．可逆的な計算機を如何に作るかを説明し，コンピュータ科学にとっても量子計算と量子情報にとっても，これが如何に重要かを説明する．3.3節では章の最後としてコンピュータ科学の全分野を広く見渡し，量子計算と量子情報に特に関連する事項に焦点を当てる．

3.1 計算モデル

… アルゴリズムはプログラム言語から離れて存在する概念である．
— Donald Knuth

何かのタスクをするときの**アルゴリズム** (algorithm) とは何であろうか？ 子供のときにどんな大きな数でも2つの数を足し合わせる手順を学んだ．これはアルゴリズムの例である．アルゴリズム概念の基礎を数学的に正確に作ることが本節の目的である．

歴史的にアルゴリズムの概念は数世紀も遡る．大学生は2つの正の整数の最

大公約数を見付ける2千年前の Euclid のアルゴリズムを学ぶ．しかし Alonzo Church, Alan Turing 等，コンピュータ時代の先駆者達によってアルゴリズムの理論，したがって計算の近代的理論が導入されたのは1930年代になってからである．この業績は，20世紀初頭の偉大な数学者 David Hilbert によりなされた初期の深遠な挑戦に相呼応して，生み出された．Hilbert は，原理上すべての数学問題を解くことができるアルゴリズムが存在しないか，という疑問を抱いた．Hilbert は**解決問題** (Entscheidungsproblem) と呼ぶこの疑問に対する答えが yes であると期待していた．

驚いたことに Hilbert の挑戦への答えは no であることがわかった．すべての数学問題を解くアルゴリズムは存在しないのである．これを証明するために Church と Turing は，アルゴリズムの直観的概念を使うときに我々が意味するものを数学的定義に取り入れるという，奥深い問題を解かねばならなかった．これにより彼らはアルゴリズムの近代的理論と，コンピュータ科学の近代的理論の基礎を築いたのである．

本章では計算理論に対して表面上異なる2つのアプローチを用いる．第1のアプローチは Turing によって提唱されたものである．Turing は計算タスクを行うアルゴリズムという考えを取り入れるために，今日 **Turing 機械** (Turing machine) と呼ばれるクラスの機械を定義した．3.1.1項では Turing 機械について述べた後，Turing 機械モデルの幾つかの簡単な変形について議論する．第2のアプローチは計算の**回路モデル**を通じたアプローチであり，これは後で量子コンピュータを研究する準備として特に便利なものである．回路モデルは3.1.2項で述べる．これら計算モデルは表面上別物のように見えるが実は等価であることがわかっている．なぜ1つ以上のモデルを使うのか？と読者は尋ねるかも知れない．その理由は異なるモデルを使うと，特定の問題の解に対して異なる見通しが得られるかも知れないからである．ある概念に対して2つ（あるいはそれ以上）の思考方法があることは1つよりも優れている．

3.1.1　Turing 機械

Turing 機械の基本要素を図3.1に示す．Turing 機械には主要要素が4つある．

(a) **プログラム：** 通常のコンピュータに類似している．

b) **有限状態制御：** マイクロプロセッサの中心部に似た動作をする．機械の他の動作と協調して動く．

c) **テープ：** コンピュータメモリに似た動作をする．

d) **読み書き用テープヘッド：** 現在読み書きできるテープ位置を示す．

これら 4 要素について次に詳しく述べる．

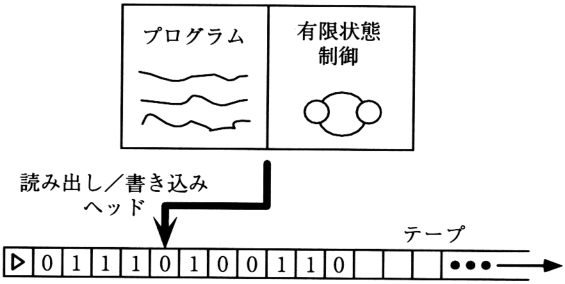


図 3.1: Turing 機械の主要要素．文中ではテープの空白は「b」で示している．テープ上の ▷ はテープ左端を表す．

Turing 機械の**有限状態制御** (finite state control) は**内部状態** (internal state) $q_1, \ldots, q_m$ の有限集合より成る．状態数 m は変更することができる．m が十分大きいとこれは機械の性能に本質的な影響を及ぼさないことがわかっているので，m がある固定した定数であるとしても一般性を失わない．有限状態制御を考える良い方法は，これを Turing 機械の動作と協調して動く一種のマイクロプロセッサと見なすことである．これはテープと別の一時記憶と，機械のための全処理を行う中心としての機能を果たす．状態 $q_1, \ldots, q_m$ の他に q_s, q_h で表される 2 つの特別な状態が存在し，これらをそれぞれ**出発状態** (starting state)，**停止状態** (halting state) と呼ぶ．この考えは計算開始時には Turing 機械は出発状態 q_s にあり，計算を行うと Turing 機械の内部状態が変化をし始める．計算が終わるときには Turing 機械が状態 q_h となり，機械が動作を完了したことを示す．

Turing 機械の**テープ**は 1 次元で一方向に無限長に伸びている．テープは無限に連なった**テープ区画** (tape square) より成っている．テープ区画に $0, 1, 2, 3, \ldots$ と番号を付ける．各区画には有限個数の異なる記号である**アルファベット** Γ から取り出した記号を 1 つ収容する．取りあえずアルファベットには 4 つの記号があるとして，それを $0, 1, b$（「空白」記号）およびテープの左端を示す ▷ で表す．最

初にテープは左端に $\triangleright$，有限個数の 0 と 1，そして残りは空白となっている．**読み書き用テープヘッド**は機械がアクセスする区画として Turing 機械テープ上の 1 テープ区画を指定する．

まとめると有限状態制御が状態 q_{s} で，読み書き用ヘッド位置がテープ左端の 0 が入った区画から機械は動作を開始する．そこから計算は以下に示すように**プログラム**に従って 1 ステップずつ進んで行く．状態が q_{h} となれば計算が停止し，そのときのテープ位置の（空白でない）テープ内容が計算の**出力**となる．

Turing 機械の**プログラム**は $\langle q, x, q', x', s\rangle$ の形に配列された有限の**プログラム行** (program line) のリストである．プログラム行の最初の項目 q は機械の内部状態集合の 1 つの状態である．第 2 の項目 x はテープ上に現れるアルファベット記号 Γ からとったものである．プログラムは次のように動作する．Turing 機械は配列されたプログラム行のリストを各マシンサイクル毎に順に通覧して，現在の機械の内部状態が q でありテープ上で読み取る記号が x であるような行 $\langle q, x, \cdot, \cdot, \cdot\rangle$ を探す．そのようなプログラム行が見付からないときは機械の内部状態は q_{h} に変化して動作を停止する．そのプログラム行が見付かればそれを**実行**する．プログラム行は次のようなステップで実行する：機械の内部状態を q' に変化し，テープ上の記号 x を x' で上書きし，s が -1，$+1$，0 のいずれであるかによってテープヘッドを左，右，そのままの位置に動かす．このルールの唯一の例外はテープヘッドがテープ区画の左端にあるときであり，そこで $s = -1$ になるとテープヘッドはその位置で止まる．

これで Turing 機械とは何かがわかったので簡単な関数を計算するときにどう使うかを見てみよう．Turing 機械の次の例を考える．機械はテープ上の 2 進数 x から出発して次に空白が続くとする．機械には出発状態 q_{s}，停止状態 q_{h} の他に内部状態 q_1, q_2, q_3 があるとする．プログラムには次のようなプログラム行があるとする．(左側の番号は後の議論で参照する便宜上付けたもので，プログラムの一部ではない．)

$$1 : \langle q_{\mathrm{s}}, \triangleright, q_1, \triangleright, +1\rangle$$

$$2 : \langle q_1, 0, q_1, b, +1\rangle$$

$$3 : \langle q_1, 1, q_1, b, +1\rangle$$

$$4 : \langle q_1, b, q_2, b, -1\rangle$$

$$5 : \langle q_2, b, q_2, b, -1\rangle$$

$$6 : \langle q_2, \triangleright, q_3, \triangleright, +1\rangle$$

$$7 : \langle q_3, b, q_{\mathrm{h}}, 1, 0\rangle.$$

このプログラムは何の関数を計算するものだろうか？ 最初機械は状態 q_{s} つまりテープ左端にあり，1 行目 $\langle q_{\mathrm{s}}, \triangleright, q_1, \triangleright, +1\rangle$ を実行する．その結果テープヘッドはテープを書き換えることなく右に動き，機械の内部状態を q_1 に変更する．プログラムの次の 3 行は次のことを保証している．機械が状態 q_1 にあるとき，テープヘッドがテープ上で 0 でも（2 行目）1 でも（3 行目）幾つでも読みながら右に動き続け，テープ内容を空白に書き換えて状態 q_1 で留まる．この動きはテープが空白の区画に達すると止まり，そこではテープヘッドは 1 区画左に動き内部状態を q_2 に変化する (4 行目)．5 行目が保証するのは空白を読むとテープ内容を書き換えることなくテープヘッドは左に動き続ける．この動きはテープヘッドが出発点に戻ると終了し，そこでテープ上の $\triangleright$ を読み取る．このとき内部状態を q_3 に書き換えて 1 区画右に移る（6 行目)．7 行目はプログラムの最後であり，テープ上に 1 を書き込んで機械は停止する．

上記の解析に拠ればこのプログラムは一定値の関数 $f(x) = 1$ を計算する．つまりテープ上でどんな数が入力されようとも数 1 が出力される．さらに一般的に Turing 機械は負でない整数から，負でない整数を得る関数を計算するものと考えられる．テープの初期状態が関数への入力を表すのに用いられ，テープの最終状態が関数の出力を表すのに用いられる．

この簡単な関数を計算するのに，Turing 機械を使うとまるで大きなトラブルに巻き込まれたかに見える．Turing 機械を使ってもっと複雑な関数を構築できるのだろうか？ 例えば入力として間を空白で区切った 2 つの数 x と y をテープ上に置いたときに，和 $x + y$ をテープ上に出力する機械を構成することができるか？ もっと一般的に Turing 機械を使ってどんなクラスの関数を計算できるのか？

計算の Turing 機械モデルを使うと，非常に多くの種類の関数を計算できることがわかっている．例えばすべての基本的算術演算，テープ上のビット列で表されるテキストの検索，その他興味ある多くの演算をするのに使える．驚くことに現代のコンピュータで行うすべての演算を Turing 機械を使ってシミュレートできる！ 実際 Church と Turing により独立に発表された論文によれば，Turing 機械の計算モデルはアルゴリズムを使った関数計算の考えを**完全に内包**している．これを **Church-Turing の提唱** (Church-Turing thesis) と呼ぶ．

> Turing 機械で計算可能な関数のクラスはアルゴリズムで本来計算可能と見なされる関数のクラスと厳密に対応する．

Church-Turing の提唱は厳密な数学的概念 — Turing 機械で計算可能な関数 — とアルゴリズムによって計算可能な関数という直観的考えとが等価であると主張するものである．この提唱は 1936 年以前には漠然とした考えであった実世界のアルゴリズムを，数学で厳密に研究できるものに変えたという事実からその重要性が認められるに至った．この重要な点を理解するために，実解析における**連続関数**の定義を考えるのが有用であろう．どんな子供でも紙の上に書いた線が連続だということはわかるが，その直観を厳密な定義にどう取り入れるかは明白というにはほど遠い．19 世紀の数学者達はいろいろな連続の定義の利点を長い間議論した末に，近代的な連続の定義を受け入れた．連続とか計算可能のような基本的定義をするときに，良い定義を選び直観的考えが正確な数学的定義と密接に適合することが重要である．この観点から Church-Turing の提唱の主張するところを要約すると，Turing 機械の計算モデルは直観的アルゴリズムの概念を厳密な定義に取り入れて，コンピュータ科学に優れた基礎を与えるものであった．

直観的にアルゴリズムで計算可能と見なすすべての関数が，Turing 機械を使って計算できるということは，必ずしも先験的に明白ではない．Church や Turing その他多くの人々が Church-Turing の提唱に対する根拠を見出すのに多くの時間を費やしたが，60 年経ってもその反証は見い出せていない．それにもかかわらず将来我々は，Turing 機械上で計算できない関数を計算するプロセスを，自然界に見出すであろう．これがもし起きれば，それまでできなかった新しい計算プロセスが強化されるので，それは素晴らしいことである．もちろん我々は計算可能性の定義と，それを使うコンピュータ科学の定義を徹底的に見直す必要があろう．

演習 3.1:（自然界の計算不能なプロセス） Turing 機械で計算可能でない関数を自然界で計算するプロセスがあったとすると，我々はそれをどのようにして認識するか？

演習 3.2（Turing 数） 単一テープを持つ複数の Turing 機械の各々にリスト 1，2，3,... の中から数字を割り振り，その数字で機械が一意に区別できることを示せ．この数を対応する Turing 機械の **Turing 数** (Turing number) と呼ぶ．（ヒント：すべての正の整数は一意の素因数 $p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$ を持つ．ここで p_i は異なる素数，$a_1,\ldots,a_k$ は負でない整数である.）

今後の章で量子コンピュータも Church-Turing の提唱に従うことがわかる．つまり量子コンピュータは，Turing 機械が計算できるのと同じクラスの関数を計算できる．量子コンピュータと Turing 機械の差は，関数を計算する**効率**にある．Turing 機械のような古典コンピュータで可能と考えられているよりも，量子コンピュータによってはるかに効率的に計算できる関数が存在するのである．

計算の Turing 機械モデルを使って，コンピュータのプログラム言語で用いるすべての通常の概念が構築できることを，詳細にわたって示すのは本書の範囲を越える（詳しい情報は章末の「歴史と参考資料」欄を参照)．アルゴリズムの計算に使う Turing 機械を明示的に規定する代わりに，アルゴリズムを規定するときに通常我々はより高次の**疑似コード** (pseudecode) を使用する．Church-Turing の提唱を信用すれば，この疑似コードは Turing 機械計算モデルに変換できる．ここで疑似コードについて厳密に定義をするのは避けるが，英語を少し形式的にした形のもの，あるいは C++や BASIC のような高級言語を少し崩した形のものと考えてよい．疑似コードを使うと，Turing 機械のような極端な詳細に立ち入ることなく，アルゴリズムを表せるので便利である．疑似コードの使用例をコラム 3.2 に示し，今後量子アルゴリズムの記述にも使用する．

基本的 Turing 機械モデルには多くの変形が存在する．異なる種類のテープを持った Turing 機械を想像することができる．例えば両方向に無限長のテープであるとか，2 次元以上の高次元のテープを使った機械が想像できるかも知れない．しかしこれまでにわかっているところでは物理学的に合理的な方法で Turing モデルの如何なる側面も変更できないし，このモデルで計算できるクラスの関数を拡張することもできない．

一例として多数のテープを備えたTuring機械を考えてみよう．より多数のテープへの拡張は容易なので，簡単のためにテープ数を2とする．基本的Turing機械と同様に，2テープTuring機械も内部状態 $q_1, \ldots q_m$ と開始状態 $q_{\rm s}$，停止状態 $q_{\rm h}$ を有する．2つのテープはそれぞれ有限のアルファベット記号 Γ から取った記号を記憶する．前と同様にアルファベットには4つの記号0, 1, b および $\triangleright$ が含まれているとするのが便利である．ここで $\triangleright$ は各テープの左端の符号である．2テープTuring機械と基本的Turing機械との主な違いはプログラムにある．プログラム行は $\langle q, x_1, x_2, q', x'_1, x'_2, s_1, s_2 \rangle$ の形をしており，その意味はもし機械の内部状態が q ならばテープ1は現在位置で x_1 を読み出し，テープ2は x_2 を読み出し，機械の内部状態を q' に変更し，x_1 を x'_1 で上書きし，x_2 を x'_2 で上書きし，テープ1とテープ2のテープヘッドは s_1 と s_2 の値が $+1$, -1, 0 に応じて，左右に移動したり現在位置に留まったりする．

どのような意味で基本的Turing機械と2テープTuring機械が等価な計算モデルなのであろうか？ 各々の計算モデルが他方を**シミュレート**できるという意味で，これら2つは等価である．2テープTuring機械においてテープ1の入力が x であるとし，両テープの残りすべてが終端記号 $\triangleright$ 以外は空白であるとする．この機械は関数 $f(x)$ を計算するものとし，$f(x)$ はTuring機械が停止したときのテープ1の内容であるとする．注目すべきは f を計算する2テープTuring機械が与えられると，それと等価な同じ関数を計算できる単一テープのTuring機械が存在する．具体的にこれをどのように行うかを陽に説明しないが，2テープTuring機械の2つのテープ内容を単一テープ上に記憶することによって，単一テープTuring機械は2テープTuring機械を**シミュレート**できる．このシミュレーションには計算上なにがしかのよけいな負担が必要であるが，重要な点は原理上常にこれができることにある．実際普遍的Turing機械が存在し（コラム3.1参照），他のいかなるTuring機械もシミュレートすることができる．

Turing機械モデルのもう1つの興味ある変形は，モデルにランダムさを導入することである．例えば次のような効果を持つプログラム行を実行するTuring機械を想像する：もし内部状態が q でテープの読みが x ならば公平にコイン投げを行う．もしコインが表なら内部状態を $q_{i_{\rm H}}$ に変え，裏ならば内部状態を $q_{i_{\rm T}}$ に変える．ここで $q_{i_{\rm H}}$ と $q_{i_{\rm T}}$ はTuring機械の2つの内部状態である．そのようなプログラムは $\langle q, x, q_{i_{\rm H}}, q_{i_{\rm T}} \rangle$ で表現される．しかし，この変形によってもTuring

機械計算モデルの本質的能力は変化しない．コイン投げの異なる値に対応する可能な計算経路をすべて明示的に「探し出す」ことにより，ランダム性を持たない通常の決定性 Turing 機械上で上のアルゴリズムをシミュレートできることを示すのは難しくない．もちろんこの決定性シミュレーションはランダムモデルに比べて効率の点で劣るかも知れないが，今の議論の主眼点はモデルにランダム性を導入することによって計算可能な関数のクラスが変化しないことにある．

演習 3.3:（ビット列を反転する Turing 機械） 2 進数入力 x を受け取り x を逆の順に出力する Turing 機械を記述せよ．（ヒント：これと次の演習では多数テープの Turing 機械を用いるか，または $\triangleright$, 0, 1 および空白以外の記号を用いるか，あるいはその両方を用いる．）

演習 3.4:（2 を法とする加法の Turing 機械） 2 つの 2 進数 x, y の 2 を法とする和を求める Turing 機械を記述せよ．これらの数は Turing 機械のテープ上に 2 進数入力 x，空白，y の順で記述する．もし一方の数のほうが長ければ短いほうの頭に 0 を補って長さを揃えてよい．

コンピュータ創始者達に最初のインスピレーションを与えた Hilbert の解決問題に話を戻そう．数学のすべての問題を決定するアルゴリズムが存在するか？この疑問に対して Church と Turing が示した答えは no であった．コラム 3.2 ではこの注目すべき事実に対する Turing の証明を説明する．この**決定不能性** (undecidability) 現象は，今では Church と Turing が構築した例をはるかに越えて拡張されている．例えば，2 つのトポロジー空間がトポロジー的に等価（位相同形 (homeomorphic)）であるかどうかを決定する問題は決定不能であることが知られている．決定不能なダイナミックなシステムの振る舞いに関連する簡単な問題を問題 3.4 で示す．これをはじめその他の例に対する参考文献は章末の「歴史と参考資料」欄に示している．

それ自身への興味はさておいて，決定不能性はコンピュータ科学および量子計算と量子情報の重要関心事を前もって示している．つまり容易に解ける問題と解くのが困難な問題の違いである．決定不能性は — 事実上解くのが不可能な難しい — 究極の解決困難な問題を提供している．

演習 3.5:（入力がないときの停止問題） Turing 機械 M が与えられ，機械への入力がテープ上の空白であるときに，M が停止するかどうかを決めるアルゴリズムはないことを示せ.

演習 3.6:（確率的停止問題） 確率的 Turing 機械を演習 3.2 と同じ方法で番号付けし，確率的停止関数 $h_p(x)$ を次のように定義する．つまり入力 x があると少なくとも確率 1/2 で機械 x が停止するならば $h_p(x)$ は 1，入力 x に対して確率 1/2 以下で機械 x が停止するならば 0 に等しい．すべての x に対して厳密に確率が 1/2 以上の正確さで，出力 $h_p(x)$ を与える確率的 Turing 機械は存在しないことを示せ.

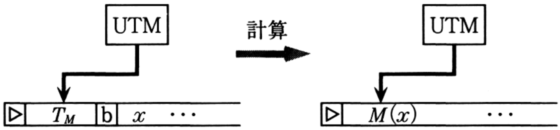
演習 3.7:（停止オラクル） 負でない整数 x を入力とし，$h(x)$ の値を出力とする**ブラックボックス** (black box) が使えるとする．ここで $h(\cdot)$ はコラム 3.2 で定義する停止関数である．このタイプのブラックボックスを停止問題に対する**オラクル** (oracle) と呼ぶ．オラクルを呼び出す能力を備えた通常の Turing 機械があるとする．これを実現する 1 つの方法は 2 テープの Turing 機械を使い，オラクルを呼び出して Turing 機械に付加的なプログラムを追加し，第 2 テープ上の現在の内容 x に対する $h(x)$ の値を第 2 テープに書き込むようにすればよい．この計算モデルは停止関数を計算できるので，明らかに従来の Turing 機械モデルより強力である．この計算モデルの停止関数は決定不能であるか？ 換言すれば停止問題のオラクルの支援を受けた Turing 機械は，オラクルを持つ Turing 機械に対するプログラムが特定の入力で停止するかどうかを決定するか？

コラム 3.1: 普遍的 Turing 機械

Turing 機械ではテープの初期形状，有限状態制御の初期状態，および機械のプログラムの 3 要素を含み，それらは機械毎に異なると述べた．**普遍的 Turing 機械** (万能 Turing 機械，UTM, universal Turing machine) と呼ぶ巧妙なアイディアでは，プログラムと有限状態制御をきっちりと固定して，テープの初期内容だけを機械の変化部分とすることができる.

普遍的 Turing 機械（下図参照）は次のような性質を持っている．M を

Turing 機械，T_M を機械 M に付随した Turing 数とする．T_M の 2 進数表現とその次に空白，その次に残りのテープ上に符号列 x が入力されると，どの機械 M であっても入力 x に対して与えるであろう出力を，普遍的 Turing 機械は出力 $M(x)$ として与える．したがって，普遍的 Turing 機械は任意の Turing 機械のシミュレーションができる．



普遍的 Turing 機械は近代的なプログラム可能なコンピュータと同様な考えに沿っている．後者でコンピュータが取るべき動作 — つまり「プログラム」— が記憶装置に蓄えられるのに類似して，ビット記号列 T_M が普遍的 Turing 機械のテープ冒頭に蓄えられる．またプログラムで処理されるデータは記憶装置の別の場所に蓄えられるが，これは普遍的 Turing 機械の x の役割と類似している．こうするとある固定したハードウェアを用いてプログラムを働かせて出力が得られる．この固定したハードウェアは普遍的 Turing 機械で実行される内部状態と（固定した）プログラムに似ている．

普遍的 Turing 機械の構成を詳細に述べるのは本書の範囲外である（勤勉な読者は構成にまで立ち入りたいかも知れないが）．重要なのはそのような機械が存在することであり，1 台の固定した機械を使ってどんなアルゴリズムでも働かすことができる点である．普遍的 Turing 機械が存在するということにより，Turing 機械の内部状態数はあまり重要でないと前に述べたことがここで説明できる．状態数 m が普遍的 Turing 機械に必要な数以上でさえあれば任意の数の内部状態を使って Turing 機械をシミュレートできるのである．

コラム 3.2: 停止問題

演習 3.2 において Turing 機械にリスト $1, 2, 3, \ldots$ の数を一意に関連づけられることを示した．Hilbert の問題を解くために Turing はこの数を使って **停止問題** (halting problem) を提起した： Turing 数 x を有する機械は

数 y が入力されると停止するか？ これは良い問題提起であり興味ある数学上の問題である．つまりこれはアルゴリズムが停止するかどうかという意味で我々にとってかなり興味がある．それなのにこの停止問題を解くことができるアルゴリズムはまだ存在しないことがわかっている．これを調べるために Turing はもう少し特殊な問題を解くアルゴリズムがないか自問した：Turing 数 x を持つ機械は同じ数 x を入力すると停止するか？ Turing は**停止関数** (halting function) を次のように定義した．

$$h(x) \equiv \begin{cases} 0, & \text{番号 } x \text{ の機械が入力 } x \text{ で停止しない場合} \\ 1, & \text{番号 } x \text{ の機械が入力 } x \text{ で停止する場合} \end{cases}$$

停止問題を解くアルゴリズムが存在するならば，$h(x)$ を計算するアルゴリズムが必ず存在するはずである．このアルゴリズム — HALT(x) と表示する — が存在するとすれば矛盾が導かれることを示そう．次の疑似コードで関数 TURING(x) を計算するアルゴリズムを考える．

```
TURING(x)
 y = HALT(x)
 if y = 0 then
        halt
 else
        loop forever
 end if
```

HALT が正当なプログラムであるためには，TURING もある Turing 数 t を有する正当なプログラムでなければならない．停止関数の定義により入力 t で TURING が停止するときにのみ $h(t) = 1$ となる．しかし TURING のプログラムを調べると，TURING が入力 t で停止するのは $h(t) = 0$ のときのみである．したがって，$h(t) = 0$ のときにのみ $h(t) = 1$ となり矛盾する．したがって，$h(t) = 0$ を計算するアルゴリズムが存在するという最初の仮定が間違っていたことになる．結論として停止問題を解くアルゴリズムは存在しない．

3.1.2 回　路

計算デバイスとして Turing 機械は少し理想化されたモデルであった．実際のコンピュータはサイズが**有限**であるのに，Turing 機械はサイズの限界がないと仮定されていた．本項ではもう 1 つの計算モデルである**回路モデル**について調べる．回路モデルは計算能力の点で Turing 機械と等価であり，多くの応用に対してより便利で現実的である．特に計算の回路モデルは量子コンピュータの準備のために重要である．

回路モデルは情報を伝達し簡単な計算タスクを実行する**配線** (wire) と**ゲート** (gate) よりなっている．例えば，図 3.2 は 1 ビット入力 a をとる簡単な回路を示しており，NOT ゲートを通るビットを 1 から 0 へ，0 から 1 へ反転させる．NOT ゲート前後の配線は NOT ゲート入出力として働き，空間を通じあるいは時間を経過したビットの動きを表す．

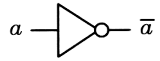


図 3.2: 入力 1 ビットに対して NOT ゲートを実行する基本回路．

一般的に回路には多くの入出力ビット，配線，論理ゲートが含まれるかも知れない．**論理ゲート** (logic gate) はある定数 k の**入力ビット**からある固定数 l の**出力ビット**への関数 $f : \{0,1\}^k \to \{0,1\}^l$ である．例えば，NOT ゲートは 1 入力ビット，1 出力ビットのゲートであり，関数 $f(a) = 1 \oplus a$ を計算する．ここで a は単一のビット，$\oplus$ は 2 を法とする和 (modulo 2 addition) を表す．不安定性を避けるために図 3.3 に示すようなループは回路内に許されないのが通例である．このような回路を**非巡回的** (acyclic) であるといい，我々も慣用を守って，計算の回路モデルは非巡回的であるとする．

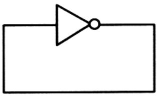


図 3.3: 巡回を含む回路は不安定となり，計算の回路モデルでは通常許容されない．

この他にも計算に有用な多くの基本的論理ゲートがある．このリストには AND ゲート，OR ゲート，XOR ゲート，NAND ゲート，NOR ゲートなどが含まれる．

これらはいずれも 2 入力ビットに対して 1 出力ビットを生み出す．AND ゲートは 2 入力が両方とも 1 であるときにのみ 1 を出力する．OR ゲートは少なくとも一方の入力が 1 であるときにのみ 1 を出力する．XOR ゲートは入力の 2 を法とする和を出力する．NAND と NOR ゲートはそれぞれ入力の AND と OR をとり，出力の如何を問わず NOT を適用した値が出力となる．これらゲートの働きを図 3.4 にまとめた．

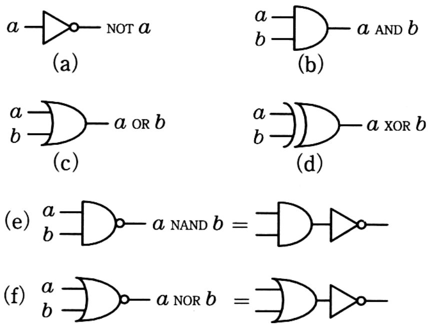


図 3.4: AND，OR，XOR，NAND および NOR ゲートを実行する基本回路．

図 3.4 に示されていない重要な回路が 2 つある．つまり，ファンアウトゲートと (FANOUT gate) と交差ゲート (CROSSOVER gate) である．ビットを「分割」して 1 ビットを 2 つのコピーで置き換える演算を FANOUT と呼ぶ．またビットを交差，つまり 2 つのビットを入れ替える CROSSOVER を許容する．図 3.4 に載っていない 3 番目の演算は実際には論理ゲートではないが，別の**補助ビット** (ancilla bit) あるいは**作業ビット**を準備して計算途中で別の作業空間をつくることである．

これら簡単な回路要素を組み合わせて数え切れない種類の計算を行うことができる．これらの要素を組み合わせると如何なる関数でも計算できることを以下に示す．その前に簡単な例として，世界中の小学生に教えられるのと本質的に同じアルゴリズムを用いて，n ビットの 2 つの整数の和を取る回路を示そう．この回路の基本要素を**半加算器** (half-adder) と呼び，図 3.5 に示す．半加算器は 2 つのビット x と y を入力として，出力 $x \oplus y$ modulo 2 と，x と y の両方が 1 ならば 1，そうでなければ 0 の桁上げビット c を与える．

図3.6 に示すように半加算器 2 つをカスケードに接続すると**全加算器** (full-adder)

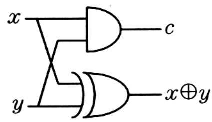


図 3.5: 半加算器回路．桁上げビット c は x と y の両方が 1 ならば 1，そうでなければ 0 である．

を構成できる．全加算器は x, y, c の 3 ビットを入力とする．x と y のビットは加え合わせるデータと考えられ，c は前の計算で得られた桁上げビットである．回路出力は 2 ビットあり，一方の出力は 3 入力全部の 2 を法とする和 $x \oplus y \oplus c$ である．2 番目の出力 c' は桁上げビットであり 2 つあるいはそれ以上の入力が 1 ならば 1，それ以外は 0 である．

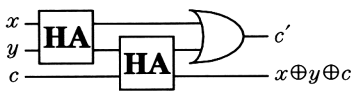


図 3.6: 全加算回路．HA は半加算器．

これらの全加算器を多段にカスケード接続すると n ビットの 2 整数を加える回路ができる．図 3.7 は $n = 3$ の場合を示す．

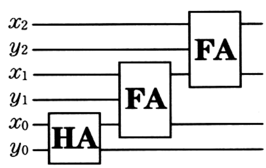


図 3.7: 小学生向けアルゴリズムを用いた 2 つの 3 ビット整数 $x = x_2x_1x_0$，$y = y_2y_1y_0$ の加算回路．HA は半加算器，FA は全加算器．

少数の決まったゲートだけを使って任意の関数 $f : \{0,1\}^n \to \{0,1\}^m$ を計算できると前に述べた．ここで n ビット入力で 1 ビット出力の簡単な場合 $f : \{0,1\}^n \to \{0,1\}$ についてこれを証明する．このような関数を **Boole 関数** (Boolean function) と呼び，対応する回路を **Boole 回路** (Boolean circuit) と呼ぶ．Boole 関数の特別な場合を証明すると，一般の場合の普遍的証明はすぐにできる．証明は n に関して帰納法で行う．$n = 1$ では関数には 4 つの可能性があり，回路が 1 本の配線からなる恒等関数，1 個の NOT ゲートで実行されるビット反転関数，入力と初期状態 0 のビットの AND で得られる入力ビットを 0 で置

き換える関数，入力と初期状態1のビットのORで得られる入力ビットを1で置き換える関数である．

帰納法を完成するためにnビットに対する任意の関数が回路で計算できるとし，fを$n+1$ビットに対する関数とする．nビット関数f_0とf_1を$f_0(x_1,\ldots,x_n) \equiv f(0,x_1,\ldots,x_n)$と$f_1(x_1,\ldots,x_n) \equiv f(1,x_1,\ldots,x_n)$で定義する．これらは$n$ビットの関数であり，帰納法の仮定によりこれらを計算する回路が存在する．

fを計算する回路を設計することは容易である．この回路は入力の最後のnビットに関する関数f_0とf_1を計算し，入力の最初のビットが0か1かに対応して適切な答えを出力する．これを実行する回路を図3.8に示す．これで帰納法の証明が完了した．

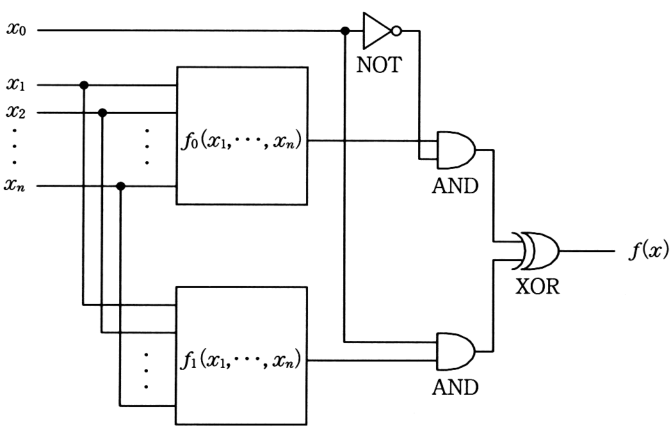


図 3.8: $n+1$ビットに対する任意の関数fを計算する回路．帰納法でnビットの関数f_0とf_1を計算する回路が存在すると仮定している．

普遍的回路を構成する要素が5つある．

(1) 配線：ビットの状態を保存する．

(2) 標準状態で用意された補助ビット：$n=1$の場合の証明に使用する．

(3) FANOUT 操作：1ビットの入力を2ビットにコピーして出力する．

(4) CROSSOVER 操作：2つのビットの値を交換する．

(5) AND，XOR，NOT ゲート．

4章（第II巻）で我々は古典回路と類似の方法で量子回路計算モデルを定義する．これら5つの要素の多くが量子回路への拡張に際して，興味深い挑戦を提起する

ことを心に留めておいて欲しい．すなわちqビットを保存するための良い量子配線を構成することは必ずしも自明ではない．非クローン化定理があるため（1.3.5項で説明したように）量子力学ではFANOUT操作を直接実行することはできない．ANDゲートやXORゲートは可逆でないので，ユニタリーな量子ゲートとして直接実現することはできない．確かに量子回路計算モデルを定義するには沢山考えるべきことがある！

演習 3.8:（NANDの普遍性） 配線，補助ビットおよびFANOUTが使えるとき，NANDゲートを用いてAND，XORおよびNOTゲートをシミュレートできることを示せ．

量子的議論に脱線したが，古典回路の性質に話を戻そう．前にTuring機械モデルは計算の回路モデルと等価であると述べた．どのような意味で両者が等価なのか？ 見たところ両モデルは全く違っているように見える．Turing機械の性質には制約がないので，アルゴリズムの意味を抽象的に規定するには便利である一方，回路のほうが実際の物理的コンピュータが行うことをきっちりと捉えている．

2つのモデルは**一様な回路族**という概念を導入すると関係付けられる．**回路族**(circuit family)とは正の整数nを指数に持つ回路の集まり$\{C_n\}$である．回路C_nはn個の入力ビット，任意の有限数の付加的な作業ビット，および出力ビットを有している．長さがたかだかnビットの数xが入力するとき，回路C_nの出力を$C_n(x)$と表す．回路に**矛盾がない**ことを要求する．つまり，もし$m < n$でxの長さがたかだかmビットならば，$C_m(x) = C_n(x)$である．回路族$\{C_n\}$で計算される関数は，xの長さがnビットならば$C(x) = C_n(x)$となる関数$C(\cdot)$である．例えばnビットの数を2乗する回路C_nを考える．こではxを任意の正の整数として関数$C(x) = x^2$を計算する回路族$\{C_n\}$が定義される．

しかし制約なしに回路族を考えるだけでは十分でない．実際のところ我々には回路を構築するアルゴリズムが必要である．もし回路族に何の制約も加えなければ，合理的計算モデルで計算できることを期待しないすべての種類の関数まで計算できてしまう．例えば$h_n(x)$は停止関数であり，xの値がnビット長に制約されているとする．したがって，h_nはnビットから1ビットへの関数であり，$h(\cdot)$を計算する回路C_nが存在することを証明した．したがって回路族$\{C_n\}$は停止関数を計算できることになる！ しかしこの回路族を使って停止関数が解けない理

由は，すべての n に対して回路 C_n を構築する特定のアルゴリズムを持ち合わせていないからである．この要請を加えると一様な回路族の概念に到達する．

n を入力すると C_n の**記述**を生成するアルゴリズムがあって，それが Turing 機械上で働くならば，回路族 $\{C_n\}$ を**一様な回路族** (uniform circuit family) と呼ぶ．つまり回路 C_n 中に含まれるゲートの記述，ゲートを結合して回路を構成する方法，回路に必要な補助ビット，FANOUT，CROSSOVER 操作，回路出力を与える配線などがアルゴリズムから生み出される．例えば上で述べた n ビットの数を 2 乗する回路族は，与えられた n に対して n ビット数を 2 乗するに必要な回路の記述を出力するので，確かに一様な回路族である．このアルゴリズムは技術者が任意の n に対して回路記述を生成できる（したがって回路を構築できる）手段と考えてよい．これと対照的に一様でない回路族を**非一様な回路族** (non-uniform circuit family) と呼ぶ．任意の n に対して回路を構築するアルゴリズムは存在せず，技術者は停止関数のように関数を計算する回路を構築することができない．

直観的に一様な回路族は何か合理的なアルゴリズムにより生成される回路の一族である．一様な回路族により計算できるクラスの関数は Turing 機械上で計算できる関数のクラスと厳密に一致する．この一様性の制約があるために Turing 機械の計算モデルの結果が通常計算の回路モデルに直接に翻訳され，またその逆も行える．後になって計算の量子回路モデルにおける一様性の問題にも，同様な注意を払わなければならない．

3.2　計算問題の解析

計算問題の解析は次の 3 つの基本的疑問に答えることである：

(1) **計算問題とはなにか？**　2 つの数を掛け合わせるのが計算問題なら，人間の詩の創作能力を越えるコンピュータプログラムを作ることも計算問題である．計算問題の解析の一般理論を発展させるために，**決定問題**(decision problem) と呼ばれる特別なクラスを取り上げて，これに焦点を絞る．この方向に集中すると簡潔かつ豊富な構造を持つ理論が展開できる．重要なことはこの理論の原理の適用範囲が決定問題に止まらないことである．

(2) **与えられた計算問題を解くためのアルゴリズムを如何に設計するか？**　問題が決まると，その問題を解くためにどんなアルゴリズムが使えるのか？ 広

いクラスの問題を解くのに使える一般的なテクニックはあるのか？ アルゴリズムが設計通りに動作するのか？

(3) **与えられた計算問題を解くために必要な最小限のリソースはなにか？** アルゴリズムを働かせるには時間，空間，エネルギーといった**リソース**が必要である．異なる状況下で1つあるいはそれ以上のリソースを最小にするのが望ましいかも知れない．問題を解決するのに必要なリソースに従って問題を分類することができるか？

次の数節ではこれらの疑問，特に (1) と (3) の疑問について調べる．1番目の「計算問題とは何か？」という疑問は最も基本的疑問なので答えを3.2.3項まで延期することとし，最初に3.2.1項でリソースの定量化に関する予備概念を確立し，次に3.2.2項で**計算量**の主要概念を概観する．

良いアルゴリズムを如何に設計するかという疑問 (2) は多くの研究者が膨大な量の独創的研究を行った主題である．それはあまりに多いので，この短い紹介では良いアルゴリズムの設計に用いられる主要概念の記述を始めることすら難しい．この素晴らしいテーマに興味を持つ読者は，章末の「歴史と参考資料」欄を参照されたい．この話題は後で量子アルゴリズムを学ぶときに直接接することになる．量子アルゴリズムを作成する技術には，古典コンピュータ向けのアルゴリズム設計の既存の概念と，新たな量子力学的アルゴリズム設計技術の両方が含まれている．この理由と，量子アルゴリズム設計が多くの点で古典アルゴリズム設計と類似している理由から，少なくともアルゴリズム設計の基本概念に精通しておくことを勧める．

与えられた計算問題を解くに必要な最小限のリソースは何かという疑問 (3) が次の数項の主題である．例えば長さ n ビットの2つの数があり，これを掛け合わせるとする．乗算を単一テープの Turing 機械で行うとすれば，計算を完成するのに Turing 機械でどれほどの計算ステップを実行しなければならないか？ 計算を終えるまでに Turing 機械上でどれだけの空間が用いられるか？

これらがリソースに関して我々が持っている疑問である．一般的にコンピュータは多くの異なるリソースを利用しているが，我々は時間，空間，エネルギーに焦点を絞る．従来コンピュータ科学では時間と空間がアルゴリズム研究の2つの主要リソースの関心事であり，これらについて3.2.2項から3.2.4項で調べる．エネルギーの重要性は少し下がるが，エネルギー要求条件の研究が可逆な古典コン

ピュータの動機となり量子計算の必要条件でもあるので，3.2.5 項でかなり詳しく計算に関するエネルギー条件について調べる．

3.2.1　計算リソースの定量化

計算モデルが異なると，計算に対して要求されるリソースも違ってくる．1 テープから 2 テープに変えるというような簡単な変化でも，計算問題を解くために Turing 機械に必要なリソースは変化するかも知れない．例えば整数の和のように非常によく理解されている計算タスクにおいても，計算モデル間のそのような変化は興味がある．しかし始めに一通り問題を理解するために，比較的些細な計算モデルの変化と無関係なリソース要求の定量化を行う．これを行うツールの 1 つが**漸近表示** (asymptotic notation) であり，これを関数の**本質的**振る舞いをまとめるのに用いる．例えば正確な時間数を気にせずに，与えられたアルゴリズムを走らせるのに本質的に何ステップかかるかを漸近表示を使ってまとめる．本項ではこの表示を詳しく述べて，計算リソースの定量化を例示する簡単な問題 — 名前リストをアルファベット順に並べ替えるアルゴリズムの解析 — に適用する．

例えば 2 つの n ビット数を足し合わせるのに必要なゲート数に興味を持つとする．必要ゲート数を正確に数えても大きな全体像がぼやけてしまう — 多分このタスクを行う特定のアルゴリズムでは $24n + 2\lceil \log n \rceil + 16$ 個のゲートが必要であろう．しかし問題のサイズが大きい極限では重要になるのは $24n$ の項である．さらにアルゴリズムの解析には定数因子は 2 次的重要性しかないので無視する．そうするとアルゴリズムの**本質的**な振る舞いは要求される演算数 n でスケーリングされるとまとめられる．ここで n は加えられる数のビット数である．漸近表示はこの表示を正確にするための 3 つのツールからなっている．

記号 O（「大文字のオー」）は関数の振る舞いの**上界** (upper bound) を設定するのに用いる．$f(n)$ と $g(n)$ は負でない整数に依存する 2 つの関数とする．c と n_0 を定数として，もし n_0 より大きなすべての n に対して $f(n) \leq cg(n)$ ならば「$f(n)$ はクラス $O(g(n))$ の関数である」，あるいは単に「$f(n)$ は $O(g(n))$ である」という．つまり十分大きな n に対して関数 $g(n)$ は重要でない定数因子を除いて $f(n)$ の上界である．アルゴリズムが使うリソースの上界を知ることで十分な場合に，大文字の O 記号は**特定の**アルゴリズムの最悪ケースの振る舞いを調べるのに

特に便利である．

アルゴリズムの**クラス**— 例えば2つの数を掛けるアルゴリズムの全クラス —の振る舞いを調べるときに，必要なリソースの下界を設定することが重要である．このために Ω（「大文字のオメガ」）記号が用いられる．n_0 より大きなすべての n に対して $cg(n) \leq f(n)$ となるような c と n_0 が存在するとき，関数 $f(n)$ は $\Omega(g(n))$ であるという．つまり十分大きな n に対して重要でない定数因子を除いて $g(n)$ は $f(n)$ の下界である．

最後に，Θ（「大文字のシータ」）記号を用いて，重要でない定数因子を除いて $f(n)$ が漸近的に $g(n)$ と同じ振る舞いをすることを表す．つまり $f(n)$ が $O(g(n))$ であると同時に $\Omega(g(n))$ であるならば，$f(n)$ は $\Theta(g(n))$ であるという．

漸近表示：例

漸近表示の簡単な例を二三考えよう．関数 $2n$ はすべての正の n に対して $2n \leq 2n^2$ なのでクラス $O(n^2)$ である．関数 2^n は十分大きな n に対して $n^3 \leq 2^n$ なので $\Omega(n^3)$ である．最後に関数 $7n^2 + \sqrt{n}\log(n)$ は十分大きな n に対して $7n^2 \leq 7n^2 + \sqrt{n}\log(n) \leq 8n^2$ なので $\Theta(n^2)$ である．次の演習ではアルゴリズム解析に便利なツールとなる漸近表示の基本的性質を幾つか練習する．

演習 3.9: $g(n)$ が $\Omega(f(n))$ であるときにのみ $f(n)$ は $O(g(n))$ であることを証明せよ．$g(n)$ が $\Theta(f(n))$ であるときにのみ $f(n)$ は $\Theta(g(n))$ であることを導け．

演習 3.10: $g(n)$ は次数 k の多項式であるとする．任意の $l \geq k$ に対して $g(n)$ は $O(n^l)$ であることを示せ．

演習 3.11: 任意の $k > 0$ に対して $\log n$ は $O(n^k)$ であることを示せ．

演習 3.12:（$n^{\log n}$ **は超多項式的 (super-polynomial) である**） 任意の k に対して n^k は $O(n^{\log n})$ であるが，$n^{\log n}$ は決して $O(n^k)$ でないことを示せ．

演習 3.13:（$n^{\log n}$ **は劣指数関数的 (sub-exponential) である**） 任意の $c > 1$ に対して c^n は $\Omega(n^{\log n})$ であるが，$n^{\log n}$ は決して $\Omega(c^n)$ でないことを示せ．

演習 3.14: $e(n)$ は $O(f(n))$ で $g(n)$ は $O(h(n))$ であるとする．$e(n)g(n)$ は $O(f(n)$ であることを示せ．

リソースの定量化における漸近表示の用例として，n 個の要素を持つ名前リストをアルファベット順に分類する簡単な応用問題を例に示す．多くのソーティングアルゴリズムは「比較と交換」(compare-and-swap) 演算を基礎としている．つまり n 要素のリスト中から 2 つの要素を比較し順序が違っていれば入れ替える．もしこの「比較と交換」演算がリストを操作する唯一の方法だとすれば，リストを正しくソーティングするに必要な演算回数はどれくらいか？

ソーティング問題を解くための単純な比較と交換アルゴリズムは次の通りである：(compare-and-swap(j, k) は j 番目と k 番目の要素を比較して順序が違っていれば入れ替える演算である.）

```
for j = 1 to n - 1
        for k = j+1 to n
                compare-and-swap(j, k)
        end k
end j
```

このアルゴリズムが n 個の名前のリストをアルファベット順に正しくソーティングすることは明らかである．アルゴリズム中の「比較と交換」演算の実行回数は $(n-1)+(n-2)+\cdots+1=n(n-1)/2$ である．したがって，アルゴリズム中で使われた「比較と交換」演算の数は $\Theta(n^2)$ である．これよりうまくできるであろうか？ うまくできることがわかっている．「ヒープソート」と呼ばれるアルゴリズムを使うと $O(n\log n)$ 回の「比較と交換」演算で済む．さらに演習 3.15 では「比較と交換」演算に基づく任意のアルゴリズムで $\Omega(n\log n)$ 回の演算で済むような簡単な計数法を議論する．したがって，一般にソーティングには $\Theta(n\log n)$ 回の「比較と交換」演算が要求される．

演習 3.15: **(「比較と交換」を基礎にいたソーティングの下界)**　n 個の要素を持つリストに対して，何か一連の「比較と交換」演算を適用してソーティングを行うとする．リストの最初の配列には $n!$ 個の可能な配列がある．「比較と交換」演算を k 回適用すると最初の可能な配列のうちでたかだか 2^k 個が正しい順序に配列されることを示せ．すべての可能な初期配列を正しい順

序にソーティングするに必要な「比較と交換」演算の回数は $\Omega(n \log n)$ である，という結論を導け．

3.2.2 計算量

それを解くアルゴリズムがないであろうという考え—これは決して変わらない何か基本的なもの —こういう考えが私に訴え掛ける．
— Stephen Cook

ときどき何か不可能なことがあるのは悪くない．私に対して誰もできないことが沢山あるというのはうれしいことだ． — Leonid Levin

多項式アルゴリズムを「実際上効率的な計算」の非公式概念を意味すると数学的概念として選択することがあらゆる側面から批判に曝されているのは驚きではない． ... 結局我々の選択に対する議論はこうあるべきである：**多項式の最悪性能を効率の基準に採用すると，その結果実際の計算に関する意義深い見通しを与え，この単純化がなければ不可能な簡潔で有用な理論が得られる．**
— Christos Papadimitriou

計算を行うにはどのような時間と空間のリソースが要求されるのか？ 多くの場合これは計算問題について我々が持つ最も重要な疑問である．数の和とか積のような問題を実行するには僅かな**空間**しか消費しない**速い**アルゴリズムがあるので，これは効率良く解けると見なされる．他の多くの問題では速いアルゴリズムが知られておらず，実行上解くのが不可能なものがある．これは問題を解くアルゴリズムが見付からないからではなく，知られているアルゴリズムがすべて膨大な量の空間または時間を消費するので，実際上使えないからである．

計算量 (computational complexity) は計算問題を解くのに必要な時間と空間リソースに関する研究である．計算量問題のタスクはアルゴリズムが明示的に知られていなくても，問題を解くことができる最良のアルゴリズムに要求されるリソースの**下界** (lower bound) を証明することである．本項と次の 2 項では計算量の主要概念やこの分野の重要な結果などについて解説する．計算量はある意味で

アルゴリズム設計分野の補足的役割である．理想的には我々に最も効率的アルゴリズムを設計できるならば，計算量で証明された下界と完全に一致するであろう．不幸にして必ずしもこうとは限らないことが多い．すでに述べたように本書では古典アルゴリズムの設計は深く追求しない．

計算量理論を定式化する際の困難な点は，同じ問題を解くにも計算モデルが異なれば要求されるリソースも異なることである．例えば多数のテープを有するTuring 機械では，実質上単一テープの Turing 機械よりも多くの問題を速く解くことができる．この困難は少し荒っぽい方法で解決される．n ビットの入力を与えて問題を規定すると考える．例えば特定の n ビット数が素数であるかどうかに関心があるとする．計算量の主な違いは n の**多項式** (polynomial) で有界なリソースを用いて解ける問題と，n の多項式より早く増大するリソースを要する問題との間で生じる．後者の場合要求されるリソースは問題のサイズに関して**指数関数的** (exponential) であるという．しかし $n^{\log n}$ のような場合には任意の多項式より早く増大する（したがって，この用語の限りでは「指数関数」である）が，任意の真の指数関数よりは遅くしか増大しないので，これは指数関数という言葉を誤用したものである．多項式リソースを用いて問題を解くアルゴリズムが存在するならば，その問題は**容易** (easy, tractable, feasible) であるといい，最良の可能なアルゴリズムが指数関数的リソースを必要とするならば**困難** (hard, intractable, infeasible) であるという．

簡単な例として $x_1 \ldots x_{m_1}$ と $y_1 \ldots y_{m_2}$ に2進数展開した2つの数があり，この2つの数の和を求めるとする．入力の全サイズは $n \equiv m_1 + m_2$ である．2つの数の和は初歩的演算を用いて $\Theta(n)$ でスケーリングするのが容易にわかる．このアルゴリズムはタスクの実行に多項式数（実際には線形数）の演算を用いる．これに対して整数を素因数に分解する問題は困難であると信じられている（けれども証明されてはいない！）．つまり信じられているのは，任意の n ビットの整数を $O(p(n))$ 回の演算で解くアルゴリズムは存在しない，ということである．ここで p は n のある決まった多項式関数である．この意味で困難と信じられている問題の他の例がこの後多数出てくる．

多項式対指数関数という分類は少し粗雑である．実際には $2^{n/1000}$ 回の演算で問題が解けるアルゴリズムは，n^{1000} 回の演算のアルゴリズムより多分有用であろう．入力サイズが非常に大きいとき（$n \approx 10^8$）にのみ，「効率的」多項式アル

ゴリズムが「非効率的」指数関数アルゴリズムより望ましいのであり，多くの目的には「非効率的」アルゴリズムを選ぶほうがより現実的かも知れない．

それにもかかわらず計算量のベースを主として多項式対指数関数の分類に置くには多くの理由がある．第1に歴史的に二三の例外を除いて，多項式リソースアルゴリズムは指数関数的アルゴリズムより格段に速かった．この理由は想像力の欠如であるという気がしている．n，n^2 あるいは何か他の低次多項式数の演算を見付けることは，n^{1000} 回の演算を必要とする無理のないアルゴリズムを見付けるより — そのような例が実際に存在するけれども — 容易であることが多い．人間の意向には比較的簡単なアルゴリズムを見付けやすい傾向があるため，実際に多項式アルゴリズムが指数関数よりも効率が良いとなったのである．

多項式対指数関数の分類を強調する第2のより基本的理由は**強い Church-Turing の提唱** (strong Church-Turing thesis) より導かれる．1.1 節で議論したように 1960 年代，70 年代には確率的 Turing 機械が最強の「合理的」計算モデルと見なされた．正確に言えば研究者は矛盾なく次のことを見出した：計算の確率的 Turing 機械モデルでない，何か別のモデルを用いて k 回の基本的演算で関数を計算できるならば，確率的 Turing 機械モデルを用いると同じ関数をたかだか $p(k)$ 回の演算で計算するのが常に可能である．ここで $p(\cdot)$ はある**多項式関数**である．この記述を**強い Church-Turing の提唱**と呼ぶ：

> **強い Church-Turing の提唱：** 任意の計算モデルは，必要とする基本的演算回数をたかだか多項式数増加するだけで，確率的 Turing 機械上でシミュレートできる．

強い Church-Turing の提唱は計算の確率的 Turing モデルに注目が集まることを意味していたので，計算量理論にとって大きなニュースであった．もし確率的 Turing 機械上で問題の多項式解がない場合，結局強い Church-Turing の提唱は如何なる計算デバイス上でも効率的解がないことを意味している．したがって，強い Church-Turing の提唱の意味するところは，もし効率の概念が多項式リソースのアルゴリズムで規定されるならば，計算量理論全体が簡潔でモデルに依存しない形を持つようになる．この簡潔さによって「多項式リソースで解ける」ことと「効率良く解ける」ことが同一であると受け入れられる根拠となった．もちろん量子コンピュータに関心が持たれる主な理由は，確率的 Turing 機械を含むすべ

ての古典コンピュータ上で困難と信じられている問題に対して効率的解を可能にすることによって，強い Church-Turing の提唱に疑問を投げかけたからである．それにもかかわらず強い Church-Turing の提唱がモデルに依存しない計算量理論の探求に果たした役割を理解し評価することは有益である．

最後にコンピュータ科学者の実際上の興味は，関数の多項式対指数関数分類だけにあるのでないことを指摘しておく．これは単に計算量問題の困難さを理解する最初の大まかな方法であるにすぎない．しかしこれは非常に重要な相違点であり，コンピュータ科学のリソース問題の性質について，多くの広範囲な論点を示している．本書の大部分でこれが与えられたアルゴリズムの効率評価における中心的関心事となる．

多項式対指数関数の分類の利点を調べたので，ここで計算量理論には1つ顕著な失敗があることを告白する：解くために指数関数的リソースを必要とする興味ある問題のクラスがあることを証明するのは非常に困難に見えることである．たいていの問題が指数関数的リソースを必要とすることを非構造的に証明することは極めて容易であり（演習3.16参照），さらに多くの興味ある問題を解くのに指数関数的リソースを必要とすることが**推測**されている．しかし少なくとも現在の知識では厳密な証明は非常に困難である．量子コンピュータの計算能力が**古典**計算量理論の大きな未解決問題と関係してくるので，計算量理論のこの失敗は量子計算に重要な意味を持っている．この問題を解決するまでは量子コンピュータの計算能力が如何に優れているかはおろか，古典コンピュータより優れているということさえ確信を持って言うことができない！

演習 3.16:（計算困難な問題の存在） 計算するのに少なくとも $2^n/n$ 個の論理ゲートを必要とする n 入力の Boole 関数が存在することを示せ．

3.2.3　決定問題と計算量クラス P と NP

多くの計算問題が**決定問題** (decision problem) — yes か no で答える問題 — として手際よくまとめられる．例えば与えられた数 m は素数であるか否か？ これは**素数判定** (primality) の決定問題である．計算量の主要概念はよく決定問題を通じて容易に定式化される．これには2つの理由があり，この形だと理論が簡

単で簡潔な形となり，かつ無理なく複雑な場合に一般化できる．歴史的に計算量問題は主として決定問題の研究から生まれた．

多くの決定問題が簡単で馴染み深い言語で容易に記述できるが，決定問題の一般的性質を議論するには**形式言語** (formal language) の用語が大いに役立つ．この用語では**アルファベット** Σ 上の**言語** (language) L は，Σ からの記号からなるすべての（有限）記号列の集合 Σ^* の部分集合である．例えば，もし $\Sigma = \{0, 1\}$ ならば，偶数の 2 進数表現の集合 $L = \{0, 10, 100, 110, \ldots\}$ は Σ 上の言語である．

決定問題は言語に関する問題として明らかな方法で符号化できる．例をあげると素数判定の決定問題は 2 進数のアルファベット $\Sigma = \{0, 1\}$ を使ってコード化できる．Σ^* からの記号列はそのまま負でない整数と解釈できる．例えば 0010 は数 2 と解釈できる．言語 L は対応する数が素数であるようなすべての 2 進数記号列よりなると定義する．

素数の決定問題を解くために我々が使うのは Turing 機械であり，入力テープ上で数 n が与えられて出発すると，もし n が素数ならば「yes」，素数でないなら「no」に等価な出力を最後に出す．この考えを正確にするために，我々の古い（3.1.1 項の）Turing 機械の定義を少し変形して，停止状態 q_{h} を「yes」と「no」の答えを表す 2 つの状態 q_{Y} と q_{N} に置き換える．その他のすべての点で機械は変わらない働きをして，状態 q_{Y} または q_{N} に入ると停止する．一般的に言語 L は Turing 機械により**決定**され，テープ上の入力 x が言語 L の要素であるかどうかを機械が決定して，もし $x \in L$ ならば状態 q_{Y}，$x \notin L$ ならば状態 q_{N} で停止する．2 つの出力のいずれが出るかによって機械が**受理**したとか**拒絶**したという．

数が素数であるかどうかをどれだけ速く決定できるか？ つまり素数判定の決定問題を表現する言語を決定する最速の Turing 機械は何か？ 言語中に長さが n の候補 x が存在するかどうかを時間 $O(f(n))$ 内に決める Turing 機械が存在するならば，その問題は $\mathbf{TIME}(f(n))$ にあるという．もしある有限の k に対して問題が $\mathbf{TIME}(n^k)$ にあるならば，その問題は**多項式時間** (polynomial time) で解けるという．ある k に対して $\mathbf{TIME}(n^k)$ にある全言語の集まりを $\mathbf{P}$ で表す．$\mathbf{P}$ は**計算量クラス** (complexity class) の最初の例である．一般に計算量クラスは言語の集まりで定義される．計算量理論の多くは種々の計算量のクラスの定義と，異なる計算量クラス間の関係を理解することに関与している．

驚くことではないが多項式時間では解けない問題が存在する．任意の与えられ

た問題が多項式時間で解けないことの推論は沢山あるが，不幸にして証明するのは非常に困難である．**P** にないと信じられている興味深いが困難な問題の簡単な例は**素因数分解決定問題**である：

> 素因数分解：合成数 m と $l < m$ が与えられたとき m は l より小さい意味のある因数を持つか？

素因数分解の興味ある性質は，もし誰かが答えは「yes」であると主張して m は l 以下の意味のある因数を持っているというと，その因数を示して立証することができ，別の人が単なるわり算を実行することにより効率良く検証できることである．そのような因数を我々は m が l 以下の因数を持つ事実に対する**証言**(witness)とよぶ．容易に検証できる証言があることが，以下で計算量クラス **NP** を定義する鍵となる概念である．素因数分解を決定問題と呼んだが，この決定問題は数の因数を見付けるのと等価であることが容易に証明できる：

演習 3.17: 素因数分解の決定問題が **P** に在るときにのみ，数 m の因数を見付ける多項式時間アルゴリズムが存在することを証明せよ．

素因数分解は **NP** と呼ばれる重要な計算量クラスに属する問題の一例である．**NP** の問題の特徴は，問題の「yes」の事例が適当な証言によって容易に証明できることである．厳密には Turing 機械 M が次の性質を満たすときに言語 L は **NP** に在るという：

(1) もし $x \in L$ ならば，機械 M が x - 空白 - w から出発して $|x|$ の多項式時間後に状態 q_Y で停止するような証言記号列 w が存在する．

(2) もし $x \notin L$ ならば，証言の役割をしようとするすべての記号列 w に対して，機械 M が x - 空白 - w から出発して $|x|$ の多項式時間後に状態 q_N で停止する．

NP の定義には興味深い非対称性がある．$x \in L$ への可能な証言が真の証言であることを速く決めることができなければならない一方で，$x \notin L$ への証言を作り出す必要はない．例えば，素因数分解の場合に我々は与えられた数が m 以下の因数を持つことを証明する簡単な方法を持っているが，ある数が m 以下の因数を持たないことを証明する証言を示すことには慎重になる．これより **coNP** を定

義するヒントが得られる．これは「no」の事例に対する証言を持っている言語のクラスであり，明らかに **coNP** の言語は **NP** の言語の補集合である．

P と **NP** はどのような関係にあるか？ 明らかに **P** は **NP** の部分集合である．コンピュータ科学における有名な未解決問題は **P には無くて NP には在る問題があるかどうか**，しばしば **P ≠ NP 問題**と称される問題である．たいていのコンピュータ科学者は $\mathbf{P} \neq \mathbf{NP}$ であると信じているが，10 年以上研究しても誰もこれを証明できておらず，$\mathbf{P} = \mathbf{NP}$ の可能性も残っている．

演習 3.18: もし $\mathbf{coNP} \neq \mathbf{NP}$ ならば $\mathbf{P} \neq \mathbf{NP}$ であることを示せ．

最初は推論 $\mathbf{P} \neq \mathbf{NP}$ を解くのはかなり易しいと思いがちである．なぜ実際にこれが微妙であるかを見るために，**P** と **NP** にある 2 つの問題例を見てみよう．この例は**グラフ理論**に関するである．グラフ理論には多くの決定問題があり，驚くほど多くの具体的応用がある．**グラフ** (graph) は**頂点** (vertex) $\{v_1, \ldots, v_n\}$ と，それをつなぎ頂点の対 $\{v_i, v_j\}$ で与えられる**辺** (edge) の有限な集まりである．さしあたり**無向グラフ** (undirected graph) を考え，（各辺の対における）頂点の順序は重要でないとする．同様の考えは頂点の順序を考慮する**有向グラフ** (directed graph) に対しても調べることができる．典型的グラフを図 3.9 に示す．

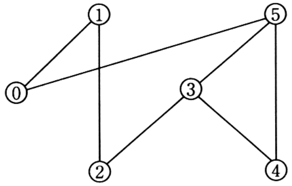


図 3.9: グラフ

グラフの**閉路** (cycle) とは，頂点対 (v_j, v_{j+1}) の辺を通る頂点の配列 $v_1, \ldots, v_m$ であり (v_1, v_m) と表す．**単純閉路** (simple cycle) とは最初と最後の頂点以外は 1 度しか通らない閉路である．**Hamilton の閉路** (Hamiltonian cycle) はグラフ中の全頂点を通る単純閉路である．Hamilton 閉路を持つグラフと持たないグラフの例を図 3.10 に示す．

Hamilton の閉路問題 (HC; Hamiltonian cycle problem) とは与えられたグラフに Hamilton 閉路が含まれるかどうかを決める問題である．与えられたグラ

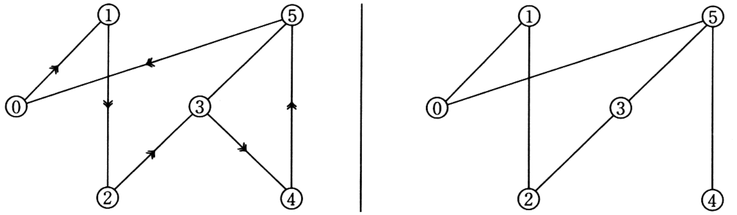


図 3.10: 左のグラフは Hamilton の閉路 $0, 1, 2, 3, 4, 5, 0$ を含む．右のグラフを見るとわかるように Hamilton の閉路を含まない．

フが Hamilton 閉路を持つならば，その閉路は簡単に検証できる証言として使えるので，HC は **NP** にある決定問題である．さらに HC には多項式時間のアルゴリズムは知られていない．実際 HC はいわゆる **NP** 完全クラスの問題である．つまり HC が時間 t で解けるとすると **NP** の他の任意の問題は時間 $O(\text{poly}(t))$ で解けるという意味で，**NP** にある「最も困難」な問題と見なされる．もし任意の **NP** 完全問題が多項式時間の解を持つならば，これもまた $\mathbf{P} = \mathbf{NP}$ となることを意味している．

Euler の閉路決定問題 (EC; Euler cycle decision problem) という問題があり，表面上は HC に似ているが，驚くほど異なる性質を持っている．**Euler の閉路** (Euler cycle) はグラフ G 中の各辺を正確に 1 回しか通らないような辺の配列である．n 個の頂点を持つグラフ G が与えられたとき，Euler の閉路決定問題 (EC) はグラフに Euler の閉路が含まれるかどうかを決定する問題である．実際 EC は HC と全く同じ問題であり，通路が頂点でなく辺である点だけが異なる．演習 3.20 で証明する次の有名な定理を考える．

定理 3.1:（Euler の定理）　連結したグラフに Euler の閉路が含まれるのは，各々の頂点に接続される辺の数が偶数の場合のみである．

Euler の定理により EC を効率良く解く手段が得られる．第 1 段階はグラフが連結されているのを調べることであり，演習 3.19 に示すように $O(n^2)$ 回の演算で容易にできる．グラフが連結されていなければ Euler の閉路が存在しないことは明らかである．グラフが連結されていれば各頂点に対して偶数個の辺があることを検証する．もしこうなっていない頂点が見付かれば Euler の閉路は存在せず，そうでなければ Euler 閉路が存在する．頂点の数が n であり辺の数がたかだか

$n(n-1)/2$ であるから，このアルゴリズムには $O(n^3)$ 回の基本的演算が必要である．したがって EC は **P** にある！ ともかく各辺を通る問題には EC の効率的アルゴリズムに利用できる構造が存在しているが，各頂点を通る問題には反映していない．このような構造が本当に HC には存在しないとすると，なぜ一方の問題にこのような構造が存在して他方の問題に存在しないのか全くわからない．

演習 3.19: REACHABILITY 問題とは，グラフ中に指定された 2 つの頂点の間に通路が存在することを決定する問題である．グラフが n 個の頂点を持つならば，REACHABILITY は $O(n^2)$ 回の演算で解けることを示せ．REACHABILITY の解を使って，グラフが $O(n^3)$ 回の演算で連結されるかどうかを決定せよ．

演習 3.20:（Euler の定理） Euler の定理を証明せよ．特に各頂点につながる辺の数が偶数ならば，Euler の閉路を見付ける建設的手続きを求めよ．

素因数分解決定問題と素因数分解問題が等価であるということは，コンピュータ科学の重要な概念である**縮約** (簡約，reduction) の 1 事例である．我々は直観的にある問題が他の問題の特別な場合であり得ることを知っている．縮約の重要な例をあげると，**巡回セールスマン決定問題** (TSP; traveling salesman decision problem) は HC の縮約である．巡回セールスマン決定問題とは次のようなものである：n 個の都市 $1, 2, \ldots, n$ と，2 つの都市対ごとに負でない整数の距離 d_{ij} が与えられたとする．距離 d が与えられるとき問題は d 以下の距離で全都市を巡る旅行が存在するかどうかを決める．

HC から TSP への縮約は次のように行う．n 個の頂点を持つグラフがあるとする．これを TSP の事例に変えるには次のように考える．グラフの各頂点を「都市」としてもし i と j が連結されていれば都市 i と j の間の距離 d_{ij} を 1 と定義し，連結されていなければ距離を 2 とする．このとき距離 $n+1$ 以下の都市の旅行ができるには距離 n でなければならず，グラフに対応する Hamilton の閉路となる．逆にもし Hamilton の閉路が存在するならば，距離 $n+1$ 以下の都市の旅行が存在しなければならない．こうして TSP を解くアルゴリズムが与えられれば，あまり手間をかけずにそれを HC を解くアルゴリズムに変えることができる．これから 2 つの結論が導かれる．1 つはもし TSP が容易な問題ならば HC も容

易である．もう 1 つはもし HC が困難ならば TSP もまた困難でなければならない．ここで HC 問題を TSP 問題に還元したがこれが**縮約**と呼ぶ一般的テクニックの例である．このテクニックは本書を通じて頻繁に利用する．

一般的な縮約の概念を図 3.11 に示す．多項式時間で演算を行う Turing 機械が存在し，与えられた入力 x に対して出力 $R(x)$ を与え，$R(x) \in A$ のときにのみ $x \in B$ ならば，言語 B は他の言語 A に**可約** (縮約可能，reducible) であるという．したがって，もし A を決定するアルゴリズムがあるならば，僅かな手間で言語 B を決定できる．この意味で言語 B は本質的に言語 A よりも決定するのが難しくない．

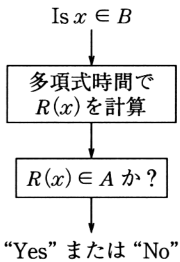


図 3.11: B から A への縮約．

演習 3.21: (縮約の移行性)　もし言語 L_1 が言語 L_2 に可約であり，言語 L_2 が L_3 に可約ならば言語 L_1 は言語 L_3 に可約であることを示せ．

ある計算量クラスにはそのクラスに関して**完全**問題 (complete problem) がある．その意味はその計算量クラス中の他のすべての言語が言語 L に縮約されるという意味で決定するのが「最も困難な」言語 L がそのクラスに存在する．全計算量クラスに完全問題があるわけではないが，我々が関心を持つ多くの計算量クラスには完全問題がある．自明な例であるが L は空集合や全単語の集合ではない $\mathbf{P}$ 中の任意の言語とする．つまり $x_1 \notin L$ なる記号列 x_1 と，$x_2 \in L$ なる記号列 x_2 が存在する．このとき $\mathbf{P}$ における他の任意の言語 L' は次の手続きで L に縮約される：与えられた入力 x に対して，多項式時間の決定手続きを用いて $x \in L'$ であるか否かを決定する．これが否ならば $R(x) = x_1$ とおき，そうでなければ $R(x) = x_2$ とおく．

演習 3.22: L がある計算量クラスで完全であり，L' はそのクラスの別の言語であって L が L' に縮約するとする．L' はその計算量クラスで完全であることを示せ．

もう少し意味のある例をあげると **NP** にも完全問題がある．このような問題の重要な例であり他の全 **NP** 完全問題の原型となっているのが，**回路充足可能性問題** (circuit satisfiability problem) 略して CSAT である：AND, OR, NOT で構成される Boole 回路が与えられたとすると，回路出力が 1 となるように回路入力を指定する値が存在するか？ つまりある入力に対して回路は**充足可能** (satisfiable) であるか？ CSAT の **NP** 完全問題は **Cook-Levin の定理** (Cook-Levin theorem) と呼ぶ．その証明の概略を説明する．

定理 3.2:（Cook-Levine の定理） CSAT は **NP** 完全である．

証明 証明は 2 つの部分から成る．最初の部分では CSAT が **NP** であることを示し，第 2 の部分で **NP** の任意の言語が CSAT に縮約されることを示す．両方の証明とも**シミュレーション**に基づいており，最初の部分は Turing 機械が回路を本質的に効率良くシミュレートできることを示し，第 2 の部分は回路が Turing 機械を本質的に効率良くシミュレートできることを示す．両方とも証明は全く簡単であるが，説明のために第 2 部分を詳しく示す．

最初に CSAT が **NP** にあることを示す．n 個の回路要素を含む回路と可能性のある証言 w が与えられると，w が回路を満たすか否かを多項式時間内に Turing 機械上で検証することは明らかに容易である．これで CSAT が **NP** にあることが立証される．

証明の第 2 部分では任意の言語 $L \in \mathbf{NP}$ が CSAT に縮約されるのを示す．つまり我々の目的は $R(x)$ が充足可能な回路であるときにのみ $x \in L$ を満たす，多項式時間で計算可能な縮約 R が存在するのを示すことである．縮約の考え方は，言語 L に対する事例と証言の対 (x, w) の検証に用いる，Turing 機械 M の動作をシミュレートする回路を見付けることである．その回路の入力変数が証言を表す．回路を充足する証言を見出すことは，M がある特定の証言 w に対する (x, w) を受け入れるのと等価であるという考えである．一般性を失うことなく構成を簡単にするために M について次の仮定を置く：

(1) M のテープのアルファベットは $\triangleright, 0, 1,$ および空白記号である．

(2) M はたかだか $t(n)$ の時間とたかだか $s(n)$ の全空間を使って動作する．ここで $t(n)$ と $s(n)$ は n の多項式である．

(3) 機械 M は実際上サイズ n のすべての入力に対して**正確に**時間 $t(n)$ を使って動作すると仮定する．これを実現するには $x = \triangleright$, 0, 1 および空白の各々に対してプログラム行 $\langle q_{\mathrm{Y}}, x, q_{\mathrm{Y}}, x, 0\rangle$ と $\langle q_{\mathrm{N}}, x, q_{\mathrm{N}}, x, 0\rangle$ を加えて，正確に $t(n)$ ステップ後に人為的に機械を停止させる．

M をシミュレートする構成の基本的考え方の概略を図 3.12 に示す．Turing 機械の各内部状態は回路の 1 ビットで表される．対応ビットを $\tilde{q}_s$, $\tilde{q}_1, \ldots, \tilde{q}_m$, $\tilde{q}_{\mathrm{Y}}$, $\tilde{q}_{\mathrm{N}}$ と名付ける．最初 $\tilde{q}_{\mathrm{s}}$ を 1 とおき，他の初期状態を表す全ビットを 0 とおく．Turing 機械のテープの各区画は 3 ビットで表され，2 ビットは現在テープ上にあるアルファベット（$\triangleright$, 0, 1 および空白）の文字を表し，1 ビットは読み書き用ヘッドがその区画を指していれば 1，そうでなければ 0 となる「フラッグ」ビットである．テープの内容を表すビットを $(u_1, v_1), \ldots, (u_{s(n)}, v_{s(n)})$，それに対応するフラッグビットを $f_1, \ldots, f_{s(n)}$ と書く．最初は u_j ビットと v_j ビットが適当に入力 x と w を表すようにおき，$f_1 = 1$，他のすべての $f_j = 0$ とおく．この他に 1 つの「グローバルフラッグ」ビット F があり，その役割は後で説明する．F の初期値を 0 とする．回路入力の全ビットは固定していると見なすが，証言を表すビット w は回路に対する変数ビットとする．

M の動作は，Turing 機械の 1 プログラム行の実行をシミュレートする「シミュレーションステップ」を，$t(n)$ 回繰り返すことにより得られる．図 3.13 に示すように，各シミュレーションステップはそれぞれのプログラム行に順番に対応する一連のステップに分割され，最後のステップでグローバルフラッグを 0 にリセットする．シミュレーションを終了するには，$\langle q_i, x, q_j, x', s\rangle$ の形のプログラム行をシミュレートするだけでよい．便宜上 $q_i \neq q_j$ とするが，$q_i = q_j$ のときにも同様の構造が成り立つ．手続きは次の通りである：

(1) $\tilde{q}_i = 1$ が成り立つことをチェックし，機械の現在の状態が q_i であることを示す．

(2) テープの各区画に対して：

　(a) グローバルフラッグが 0 に設定されていることをチェックし，Turing 機械がまだ動作していないことを確認する．

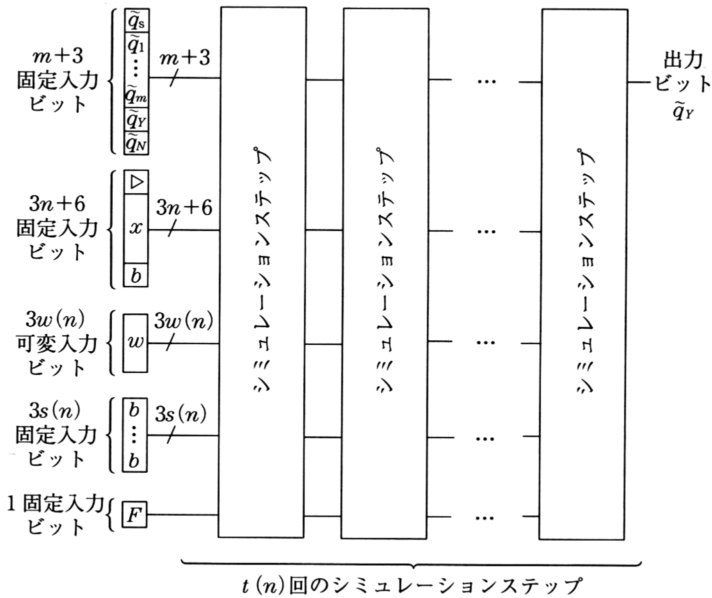


図 3.12: 回路を用いた Turing 機械のシミュレーションに使う手続きの概要.

(b) フラッグビットが 1 に設定されていることをチェックし，テープヘッドがこの区画にあることを確認する.

(c) シミュレートされるこの点のテープ内容が x であることをチェックする.

(d) 全条件のチェックが済むと，次のステップを実行する：

i. $\tilde{q}_i = 0$ と $\tilde{q}_j = 1$ に設定する.

ii. このテープの区画のシミュレートされたテープ内容を x' に更新する.

iii. $s = +1,\ 0,\ -1$，およびテープの左端にあるかどうかに対応して，ここととその隣の区画のフラッグビットを適切に更新する.

iv. グローバルフラッグビットを 1 に設定し，この一連の計算が終了したことを示す.

これは一定数のビットを含む固定した手続きであり，3.1.2 項の普遍性の結果により一定数のゲートを含む回路を用いて実行できる.

全回路中の全ゲート数は $O(t(n)(s(n)+n))$ であることが容易にわかり，これは多項式サイズである．回路の最後に機械 M が (x,w) を受け入れたときにのみ $\tilde{q}_Y=1$ となることは明らかである．したがって，w が存在して機械 M が (x,w) を受け入れるときにのみ回路は充足可能であり，L から CSAT への縮約が見出された．□

CSAT は他の多くの問題が **NP** 完全であることを証明する機会を与えてくれる．ある問題が **NP** 完全であると証明する代わりに，それが **NP** にあり CSAT がそれに縮約することを証明すればよく，もしそうならば演習 3.22 によってその問題は **NP** 完全である．コラム 3.3 において **NP** 完全問題の少数のサンプルを議論する．もう 1 つの **NP** 完全問題の例は**充足可能性問題** (SAT; satisfiability problem) であり，Boole 論理式で表現される．Boole 論理式 φ は次の要素からなっていることを思い出そう： Boole 変数の集合 x_1, $x_2,\ldots$, Boole 結合子および括弧の 3 要素である．ここで Boole 結合子 (connective) は $\wedge$ (AND), $\vee$ (OR) および $\neg$ (NOT) のような 1 または 2 入力，1 出力の Boole 関数である．与えられた Boole 変数の集合に対する真または偽は Boole 代数の通常の法則に従って決定される．例えば論理式 $\varphi=x_1\vee\neg x_2$ は充足可能な値 (assignment) $x_1=0$, $x_2=0$ を有するが，$x_1=0$, $x_2=1$ は充足可能な値ではない．充足可能性問題は Boole 論理式 φ が与えられたときに，これが可能な入力の任意の集合によって充足可能であるかどうかを決定する問題である．

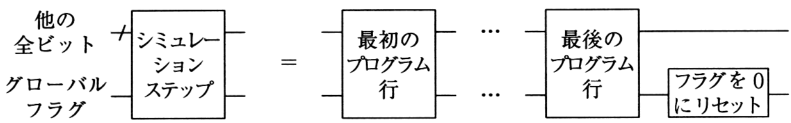


図 3.13: 回路を用いた Turing 機械のシミュレーションに使うシミュレーションステップの概要．

演習 3.23: 最初に SAT が **NP** にあることを示し，次に CSAT が SAT に縮約することを示すことによって，SAT が **NP** 完全であることを示せ．（ヒント：縮約に対して CSAT の事例の異なる配線をそれぞれ Boole 論理式の異なる変数で表すと役に立つ．）

3 充足可能性問題（3SAT）は SAT の重要な制限された重要であり，これも

NP 完全である．これは **3 論理積標準形**の論理式に関連している．論理式が 1 個あるいはそれ以上の**リテラル** (literal) の OR よりなる**節** (clause) の集まりの AND であるとき，それを論理積標準形であるという．ここでリテラルとは x または $\neg x$ の形の表現である．例えば論理式 $(x_1 \vee \neg x_2) \wedge (x_2 \vee x_3 \vee \neg x_4)$ は論理積標準形である．論理式の節が正確に 3 つのリテラルからなる場合が **3 論理積標準形** (3-conjunctive normal form) であり，**3-CNF** とも呼ぶ．例えば $(\neg x_1 \vee x_2 \vee \neg x_2) \wedge (\neg x_1 \vee x_3 \vee \neg x_4) \wedge (x_2 \vee x_3 \vee x_4)$ は 3 論理積標準形である．3 充足可能性問題は 3 論理積標準形の論理式が充足可能か否かを決定する問題である．

3SAT が **NP** 完全であることを直接証明できるが，ここで解説するには少し長すぎる．CSAT や SAT 以上に 3SAT はある意味で典型的な **NP** 完全問題であり，数え切れないほどある他の問題が **NP** 完全にあるという証明の基礎となる．**NP** 完全に関する議論の最後に，3SAT に類似で各節が 2 つのリテラルより成る 2SAT は多項式時間で解けるという驚くべき事実を指摘しておく：

演習 3.24:（2SAT は効率的解を持つ） φ は論理積標準形の Boole 論理式であり，その中の各節は 2 つのリテラルだけを含むとする．

(1) 有向辺を持つ（有向）グラフ $G(\varphi)$ を次の方法で構築せよ：G の頂点が φ の変数 x_j とその否定 $\neg x_j$ に対応する．φ に節 $(\neg\alpha \vee \beta)$ または節 $(\beta \vee \neg\alpha)$ が存在するときにのみ，G に（有向）辺 (α, β) が存在する．$G(\varphi)$ 中に x から $\neg x$ へおよび $\neg x$ から x への路 (path) があるような変数 x が存在するときにのみ，φ は充足可能でないことを証明せよ．

(2) n 個の頂点を有する有向グラフが与えられたとき，2 つの頂点 v_1 と v_2 は多項式時間で連結されるかどうかが決定できることを示せ．

(3) 2SAT を解く効率的アルゴリズムを見出せ．

コラム 3.3: NP 完全問題の動物園

クラス **NP** が重要であるのは，一部には膨大な数の計算問題が **NP** 完全であるのが知られているからである．我々はここでこの話題を概観するわけにはいかないが（「歴史と参考資料」欄を参照），多くのいろいろな数学分野

から取ってきた次の例を見れば，多くの興味深い問題が **NP** 完全として知られていることがわかる．

- CLIQUE（グラフ理論）：無向グラフ G 内のクリーク (派閥，clique) とは，すべての頂点の対が辺で連結されているものからなる頂点の部分集合である．クリークの**サイズ** (size) とはその中に含まれる頂点の数である．整数 m とグラフ G が与えられたとき G はサイズ m のクリークを持つか？
- SUBSET-SUM (算術計算)：正の整数の有限の集まり S と**標的** (target) t が与えられたとき和が t となる S の部分集合が存在するか？
- 0-1 INTEGER PROGRAMMING（線形計画法）：$m \times n$ の整数の行列 A と整数値を持つ m 次元ベクトル y が与えられたとき，$Ax \leq y$ を満たす集合 $\{0, 1\}$ の要素を持つ n 次元ベクトル x が存在するか？
- VERTEX COVER（グラフ理論）：無向グラフ G に対する**頂点被覆** (vertex cover) とは頂点の集合 V' であり，グラフのあらゆる辺の 1 つあるいは両方の頂点が V' に含まれる．整数 m とグラフ G が与えられたとき，G は m 個の頂点を含む頂点被覆 V' を持つか？

P $\neq$ **NP** と仮定すると，多項式リソースで解くことができず **NP** 完全でもない，**空でない** (non-empty) **NPI**（**NP** intermediate）問題のクラスが存在することが証明できる．明らかに **NPI** にあるとわかっている問題はないが（でなければ **P** $\neq$ **NP** であることになる)，その候補と見なせそうな問題が幾つかある．可能性の高いものを 2 つあげると素因数分解とグラフ同形性判定問題 (graph isomorphism problem) である：

> GRAPH ISOMORPHISM：G，G' は頂点 $V \equiv \{v_1, \ldots, v_n\}$ 上の 2 つの無向グラフであるとする．G と G' は同形であるか？ つまり辺 (v_i, v_j) が G に含まれるのは $(\varphi(v_i), \varphi(v_j))$ が G' に含まれるときに限るような 1 対 1 の関数 $\varphi : V \to V$ が存在するか？

NPI にある問題は量子計算と量子情報の研究者にとって 2 つの理由で興味深

い．1つには **P** にない問題を解く高速量子アルゴリズムが見付かることが望まれている．2番目には多くの人が量子コンピュータは **NP** 完全問題は別としても，**NP** にあるすべての問題も効率良く解けないであろうと疑っている．したがって，**NPI** クラスに注目が集まるのは当然である．実際に素因数分解の速い量子アルゴリズムが見付かり（5章参照），これが動機となって **NPI** にあると疑われる他の問題に対する速い量子アルゴリズムが探索されている．

3.2.4 多数の計算量クラス

重要な計算量クラスの幾つかの基本的性質を調べてきた．計算量クラスには紛れもなく華やかな集まりが存在し，これらクラス間で多くの意味のある関係が証明され，あるいは疑われている．量子計算と量子情報にとっては，定義されているすべての異なる計算量クラスを理解することは必要ない．しかし計算量クラスの中で重要なものの多くに量子計算と量子情報においても当然類似のものがあるので，その意味を認識することは有用である．さらに，もし我々が量子コンピュータの強力さを理解するならば，古典コンピュータに対して定義された多彩な計算量クラスの中で，量子コンピュータ上で解ける問題のクラスがどのように位置づけられるかを理解するのが当然である．

計算量クラスの定義で変化し得る3つの本質的性質がある：関心を持つリソース（時間，空間，...），考える問題の種類（決定問題，最適化問題，...），基礎となる計算モデル（決定的 Turing 機械，確率的 Turing 機械，量子コンピュータ，...）である．驚くまでもないがこれらにより計算量クラスの定義は広大な範囲に広がる．本項では比較的重要な計算量クラスを二三取り上げてその基本的性質を簡単に概観する．まず関心を持つリソースを時間から**空間**に変えて，定義される計算量クラスから始める．

最も自然に空間の制約を受ける計算量クラスは決定問題 **PSPACE** のクラスである．これは多項式数の作業ビットを用いて機械の使用時間量に関する制限なしに，Turing 機械上で解くことができる（演習 3.25 参照）．多項式時間後に停止する Turing 機械は多項式数のテープ区画しか横切らないので明らかに **P** は **PSPACE** に含まれるが，**NP** が **PSPACE** の部分集合であるというのも正しい．これを調べるために L を **NP** の任意の言語とする．サイズ n の問題にサイズがたかだか

$p(n)$ の証言があるとする．ここで $p(n)$ は n のある多項式である．この問題が解を持つかどうかを決定するために，$2^{p(n)}$ 個の可能な証言を順に検証する．各々の検証は多項式時間と多項式空間で行うことができる．もし検証の合間の中間作業をすべて消去するならば，全可能性を多項式空間で検証できる．

不幸にして現在のところ **PSPACE** が **P** にない問題を含んでいるかどうかわかっていない！ これはかなり注目すべき状況である — 無制限の時間と多項式空間のリソースは多項式時間だけよりも強力だというのはかなり明白である．しかしかなりの時間と工夫を投入したにもかかわらず，これは証明されていない．後で量子コンピュータ上で多項式時間で解けるクラスの問題は **PSPACE** の部分集合であることがわかる．したがって，量子コンピュータ上で効率的に解ける問題が古典コンピュータ上で効率的に解けないことが証明されれば，$\mathbf{P} \neq \mathbf{PSPACE}$ であることが確立してコンピュータ科学の大きな問題が解けることになる．この結果を楽観的に見ると，量子計算の概念が $\mathbf{P} \neq \mathbf{PSPACE}$ の証明に役立つかも知れない．悲観的に見ると，長い間経っても古典コンピュータで困難な問題を量子コンピュータで効率良く解けると厳密に証明できないという結論になるかも知れない．さらに悲観的に見ると $\mathbf{P} = \mathbf{PSPACE}$ となって，量子コンピュータは古典コンピュータに比べて利点がないことになる可能性もある！ しかし $\mathbf{P} = \mathbf{PSPACE}$ と信じている計算量の理論家は（いるとしても）ごく少数である．

演習 3.25:（$\mathbf{PSPACE} \subseteq \mathbf{EXP}$） 計算量クラス **EXP**（**指数関数時間**，exponential time）は指数関数時間つまり時間 $O(2^{n^k})$ で動作する，Turing 機械により決定されるすべての決定問題を含む．ここで k は任意の定数である．$\mathbf{PSPACE} \subseteq \mathbf{EXP}$ であることを証明せよ．（ヒント：Turing 機械に l 個の内部状態，m 文字のアルファベット，使用空間 $p(n)$ があるならば，機械はたかだか $lm^{p(n)}$ 個の異なる状態の 1 つに存在すること，および Turing 機械が無限ループを避けるならば，状態を変化させる前に停止しなければならないことを議論せよ.）

演習 3.26:（$\mathbf{L} \subseteq \mathbf{P}$） 計算量クラス **L**（**対数関数空間**，logarithmic space）は対数空間つまり空間 $O(\log(n))$ で動作し，Turing 機械によって決定されるすべての決定問題を含む．正確にはクラス **L** は 2 テープの Turing 機械を使って定義される．第 1 テープはサイズ n の問題事例を含み，テープ内容

が変化しないプログラム行だけが収容されているという意味で，読み取り専用テープである．第 2 テープは作業用テープであり，最初の内容は空白のみである．対数関数空間の要求条件は第 2 の作業用テープにだけ課されている．$\mathbf{L} \subseteq \mathbf{P}$ を示せ．

時間と空間を多く許容すると計算能力は増加するか？ この疑問への答えは両方とも yes である．大雑把に言えば**時間階層定理** (time hierarchy theorem) によって， $\mathbf{TIME}(f(n))$ は $\mathbf{TIME}\ (f(n)\log^2(f(n)))$ の真部分集合 (proper subset) である．同様に**空間階層定理** (space hierarchy theorem) によれば，$\mathbf{SPACE}\ (f(n))$ は $\mathbf{SPACE}\ (f(n)\log^2(f(n)))$ の真部分集合である．ここでもちろん $\mathbf{SPACE}\ (f(n))$ は空間リソース $O(f(n))$ で決定できるすべての言語を含む計算量クラスである．階層定理により計算量クラスの対等性に関して興味ある関連性がわかる．

$$\mathbf{L} \subseteq \mathbf{P} \subseteq \mathbf{NP} \subseteq \mathbf{PSPACE} \subseteq \mathbf{EXP}. \tag{3.1}$$

これら各々の包含関係は真であると広く信じられているが，残念ながらどれも真であると証明されていない．しかし，時間階層定理は $\mathbf{P}$ が $\mathbf{EXP}$ の真部分集合であることを示しており，空間階層定理は $\mathbf{L}$ が $\mathbf{PSPACE}$ の真部分集合であることを示している！ したがって，式 (3.1) の包含関係のうちでどれであるか不明であるが，少なくとも 1 つは真であると結論される．

ある問題が $\mathbf{NP}$ 完全であるとか何か他の困難さの条件に該当した場合にどうすればよいか？ これが決して問題解析の終わりというわけではない．1 つの可能な攻撃法は，攻撃し易いかも知れない特別な場合を見付けることである．例えば，演習 3.24 で SAT は $\mathbf{NP}$ 完全であるが，2SAT 問題 は効率的解を持つことを見た．もう 1 つのアプローチは，考えている問題のタイプを変えることであり，新たな計算量クラスを定義することになり得る戦術である．例えば，$\mathbf{NP}$ 完全問題の厳密解を求める代わりに，その問題の**近似解**を見付ける良いアルゴリズムを探すことを試みる．例えば，頂点被覆 VERTEX COVER 問題は $\mathbf{NP}$ 完全問題であるが，演習 3.27 では 2 倍以内の正確さで最小限の頂点被覆の近似解が効率良く求められることを示す．他方で問題 3.6 では $\mathbf{P} = \mathbf{NP}$ でなければ，如何なる誤差範囲でも TSP の近似解は求められないことを示す．

演習 3.27:（頂点被覆 VERTEX COVER の近似アルゴリズム） $G = (V, E)$

は無向グラフとする．次のアルゴリズムにより最小頂点被覆の2倍以内で G に対する頂点被覆が求められることを証明せよ：

```
VC = ∅
E' = E
do until E' = ∅
        let (α, β) be any edge of E'
        VC = VC ∪ {α, β}
        remove from E' every edge incident on α or β
return VC
```

なぜ1つの **NP** 完全問題の近似解を求めることができて，別の問題ではできないのか？ 結局のところ1つの問題から別の問題に効率良く変換できないのであろうか？ これは確かに可能であるが，この変換が解に対する「良い近似」であるとは限らない．その結果，**NP** の問題に対する近似アルゴリズムの計算量理論は **NP** 自身の構造を越えている．近似アルゴリズム全体の計算量理論は存在するが，残念ながら本書の範囲を超えている．しかし基本的考え方は，良い近似の概念を保存しつつ，1つの近似問題が別の問題に効率良く縮約されるように縮約の概念を定義することである．そのような考えのもとにクラス **NP** のアナロジーで，問題の近似解を効率良く確かめることができる問題の集合として，**MAXSNP** のような計算量クラスを定義することが可能である．**NP** と同様に **MAXSNP** に対して完全問題が存在し，クラス **MAXSNP** と効率良く解ける近似問題のクラスとの比較は興味ある未解決の問題である．

議論の最後に基礎となる計算モデル自身が変化したときに生じる計算量クラスについて述べる．Turing 機械がコインを投げる能力を備えており，計算の途中で取るべき行動をコイン投げの結果で決めるとする．そのような Turing 機械はある確率で入力を受け入れるかあるいは拒否できる．計算量クラス **BPP**（bounded-error probabilistic polynomial-time）はもし $x \in L$ ならば M は x を少なくとも 3/4 の確率で受け入れ，もし $x \notin L$ ならば M は x を少なくとも 3/4 の確率で拒否するような，確率的 Turing 機械 M が存在する性質を持つすべての言語 L を含んでいる．次の演習では定数 3/4 の選択は本質的に任意であることを示す．

演習 3.28:（BPP の定義における定数の任意性） k は固定した定数 $1/2 < k \leq$

1 であるとする．言語 L は $x \in L$ ならば常に M は x を少なくとも確率 k で受け入れ，$x \notin L$ ならば常に M は x を少なくとも確率 k で拒否する性質を持つ，Turing 機械が存在する言語であるとする．$L \in \mathbf{BPP}$ であることを示せ．

実際に，コラム 3.4 で議論する **Chernoff の限界** (Chernoff bound) はすべての意図と目的に対して，**BPP** にある言語を決めるアルゴリズムを数回繰り返すだけで，成功の確率が実質的に 1 に等しくなるまで増大し得ることを意味している．この理由で **P** よりもむしろ，**BPP** が古典コンピュータ上で効率的に解けると見なされる決定問題のクラスであり，量子アルゴリズムの研究で最も興味があるのは **BPP** の量子版である **BQP** (bounded-error quantum polynomial-time) である．

コラム 3.4: BPP と Chernoff の有界

確率 $1/2+\epsilon$ で正しい答えを，確率 $1/2-\epsilon$ で誤った答えを与える決定問題に対するアルゴリズムがあるとする．このアルゴリズムを n 回走らせて，最も頻繁に現れる方が正しい答えであると推測するのが合理的である．この手続きはどれくらい信頼できるか？ **Chenoff の限界**はこの疑問の答えを与える初歩的確率論の簡潔な結果である．

定理 3.3: (Chernoff の限界) $X_1, \ldots, X_n$ は独立で同等に分布したランダムな変数であり，その各々は確率 $1/2+\epsilon$ で値 1 を，確率 $1/2-\epsilon$ で値 0 をとる．このとき

$$p\Big(\sum_{i=1}^{n} X_i \le n/2\Big) \le e^{-2\epsilon^2 n}. \tag{3.2}$$

証明 たかだか $n/2$ 個の 1 を含む任意の記号列 $(x_1, \ldots, x_n)$ を考える．そのような記号列が生起する確率が最大になるのは $\lfloor n/2 \rfloor$ 個の 1 を含む場合で

ある．したがって

$$p(X_1 = x_1, \ldots, X_n = x_n) \le \left(\frac{1}{2} - \epsilon\right)^{\frac{n}{2}} \left(\frac{1}{2} + \epsilon\right)^{\frac{n}{2}} \tag{3.3}$$

$$= \frac{(1 - 4\epsilon^2)^{\frac{n}{2}}}{2^n}. \tag{3.4}$$

このような記号列がたかだか 2^n 個あり得るので，

$$p\left(\sum_i X_i \le n/2\right) \le 2^n \times \frac{(1 - 4\epsilon^2)^{\frac{n}{2}}}{2^n} = (1 - 4\epsilon^2)^{\frac{n}{2}}. \tag{3.5}$$

最後に微積分学より $1 - x \le \exp(-x)$ なので

$$p\left(\sum_i X_i \le n/2\right) \le e^{-4\epsilon^2 n/2} = e^{-2\epsilon^2 n}. \tag{3.6}$$

□

この教えるところは，固定した ϵ に対して誤った結果を与える確率は，アルゴリズムの繰り返し回数と共に**指数関数的に早く**減少する．**BPP** の場合 $\epsilon = 1/4$ なので，アルゴリズムを数百回繰り返しただけで誤りの確率を 10^{-20} 以下に下げることができる．ここまで下がるとアルゴリズムの確率に起因する誤差よりもコンピュータの部品の誤りのほうがありそうになってくる．

3.2.5　エネルギーと計算

計算量では計算問題を解くに必要な時間と空間の量を調べた．もう1つの重要な計算リソースは**エネルギー**である．本項では計算に必要なエネルギーについて調べる．驚くことに，原理上古典計算と量子計算はいずれもエネルギーを消費することなく行えるのがわかる！ 計算におけるエネルギーは計算の**可逆性** (reversibility) と深く関係している．2ビットを入力し1ビットを出力するNANDゲートのようなゲートを考える．このゲートは出力が与えられても入力は一意に決まらないので，本質的に**非可逆的** (irreversible) である．例えば，もしNANDゲートの出力が1ならば，入力は $00, 01, 10$ のいずれかであったはずである．他方NOTゲー

トは出力が与えられると入力が何であったかを推論できるので，これは**可逆論理ゲート**の例である．

非可逆性を理解するもう 1 つの方法は，情報の消去に関して考えることである．もし論理ゲートが非可逆ならば，ゲートが動作するときに入力情報の何がしかが非可逆的に失われる — つまり情報の一部がゲートで消去される．反対に可逆的計算では入力は常に出力から回復できるので，情報は消去されていない．したがって，計算が可逆であるということは，計算途中で情報が消去されないということである．

計算におけるエネルギー消費と非可逆性の関係はどうなっているか？ この関係は **Laudauer の原理** (Landauer's principle) が示しており，情報を消去するにはエネルギー消費が必要であると述べている．正確に言えば Landauer の原理は次のように表せる．

> **Landauer の原理（形式 1）**：コンピュータが情報 1 ビットを消去するとする．環境に放出される消費エネルギーの量は**少なくとも** $k_B T \ln 2$ である．ここで k_B は **Boltzmann の定数** (Boltzmann's constant) と呼ぶ普遍的定数，T はコンピュータの環境の温度である．

熱力学の法則によれば Landauer の原理はエネルギー消費ではなくエントロピーによる別の形で表せる．

> **Landauer の原理（形式 2）**：コンピュータが情報 1 ビットを消去するとする．環境のエントロピーは**少なくとも** $k_B \ln 2$ だけ増加する．ここで k_B は Boltzmann の定数である．

Landauer の原理の正当性を示すことは本書の範囲を越える物理学の問題であり，なぜ Landauer の原理が成り立つかを理解したければ，章末の「歴史と参考資料」を見て欲しい．しかし Landauer の原理を与えられたものとして受け入れれば，多くの興味ある疑問がわいてくる．まず最初に Laudauer の原理は，情報を消去する際に消費されるエネルギー量の**下界**を示しているに過ぎない．現状のコンピュータはこの下界にどれくらい近づいているだろうか？ 実はあまり近づいておらず，2000 年頃のコンピュータは各論理演算の素過程毎におよそ $500 k_B T \ln 2$ のエネルギーを消費する．

現状のコンピュータはLandauerの原理による限界からはるかに離れているが，エネルギー消費をどれくらい減らせるかを理解するのは，この原理の興味ある問題である．問題の中心的興味からはずれるが興味を持つ実際的理由はMooreの法則から来ている．もしコンピュータ能力が増加し続けるならば，演算当たりのエネルギー消費の減少が少なくともコンピュータ性能の増加と同じ割合でなければ，全消費エネルギー量も増加せざるを得ない．

もしもすべての計算が可逆的に行われるならば，可逆計算の過程ではビットは全く消去されないので，Landauerの原理はコンピュータの消費エネルギー量に下界がないことを意味している．もちろん何か他の物理原理により，計算途中にエネルギー消費が要求されるかも知れないが，幸いにしてそのようなことはない．しかし如何なる情報も消去することなく，普遍的計算が可能であろうか？ 物理学者は前もってこの疑問への答えがyesで**なければならない**ことを示して，この問題をうまく逃れることができる．なぜなら我々は現在の物理法則は基本的に可逆的であると理解しているからである．つまり，閉じた物理システムの最終状態がわかると，物理学の法則によりシステムの初期状態を知ることができる．これらの法則が正しいと信じるなら，ANDとかORのような非可逆論理ゲートに隠れて，何か基本的に可逆な計算が存在しなければならないという結論になる．しかし，隠れた可逆性とは何処にあるのか，それを使って明らかに可逆なコンピュータを構築できるのか？

2つの異なるテクニックを使って，普遍的計算ができる可逆回路に基づくモデルを作ろう．第1のモデルはビリヤードボールと反射鏡だけで構成するコンピュータであり，可逆的計算原理を見事に具体的に実現する．第2のモデルは（1.4.1項で出てきた）**Toffoliゲート** (Toffoli gate) と呼ばれる可逆ゲートに基づいており，後で量子計算の議論に大いに役立つ抽象的可逆計算の視点を提供する．普遍的計算が可能な可逆Turing機械を構築することも可能であるが，可逆回路モデルのほうが量子計算にとって遙かに有用なので，ここでは扱わないこととする．

ビリヤードボール コンピュータの基本的考えを図3.14に示す．ビリヤードボールの「入力」が左側よりコンピュータに入り，反射鏡や他の球と衝突した後，右側より「出力」として出てくる．入力位置にビリヤードボールが有るか無いかが論理的な1か0かを示す．このモデルが素晴らしいのは，その動作が古典力学の法則に基づく限り明らかに可逆的なことである．さらに標準的計算の回路モデル

における任意の計算をシミュレートできるという意味で，この計算モデルは**普遍的**である．

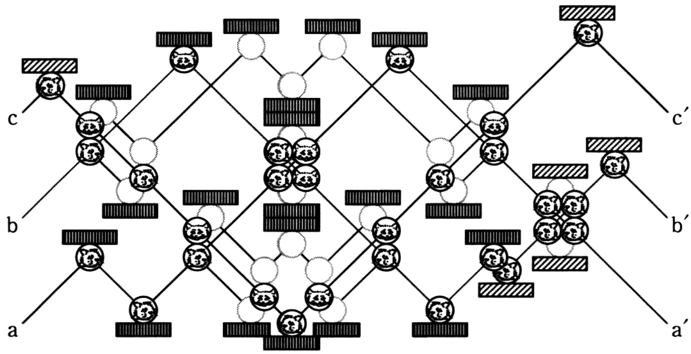


図 3.14: 3 つの入力ビットが左から入り，3 つの出力ビットが右から出てくる簡単なビリヤードボール コンピュータ．ビリヤードボールの有無が 1 または 0 を表す．空白の球は衝突により可能な進路を表す．本文で述べるようにこの特定のコンピュータは古典的な可逆 Fredkin 論理ゲートを実現したものである．

もちろんもし本当にビリヤードボール コンピュータが作られたとすると，それは非常に不安定なものになるであろう．ビリヤード競技者ならば誰でもわかるように，平滑な面上を摩擦無く転がる球は僅かな乱れで容易に進路から外れるものである．ビリヤードボールの計算モデルは，完全な動作と熱雑音のような外乱がないことを前提としている．周期的に補正をしてもよいが，本来の計算を実行するには補正によって得られる情報を消去しなければならず，仕事をする必要がある．したがって，エネルギー消費によって雑音を受ける可能性を少なくするのに役立っており，これが実世界の具体的な計算機械には必要である．ここでは紹介が目的なので，ビリヤードボール コンピュータへの雑音の影響は無視して，可逆計算の基本要素に集中することにする．

ビリヤードボール コンピュータにより，**Fredkin ゲート** (Fredkin gate) と呼ぶ可逆な普遍的論理ゲートを実現する簡潔な手段が得られる．実際可逆的ゲートと回路の一般的原理を知るために，Fredkin ゲートの性質が役に立つ．Fredkin ゲートは 3 つの入力ビットと 3 つの出力ビットを持っており，それぞれ a, b, c と a', b', c' とする．ビット c は**制御ビット**であり，その値は Fredkin ゲートの動作で変わらない，つまり $c' = c$ である．c を制御ビットと呼ぶ理由は他の 2 つ

のビット a と b の振る舞いを制御するからである．もし c が 0 ならば a と b はそのまま，つまり $a' = a$, $b' = b$ である．もし c が 1 ならば a と b は交換される，つまり $a' = b$, $b' = a$ である．Fredkin ゲートの真理値表を書き下すと図 3.15 のようになる．出力 a', b', c' が与えられると入力 a, b, c を決めることができるので Fredkin ゲートが可逆であることが容易にわかる．実際元の入力 a, b, c を得るには a', b', c' にもう 1 つの Fredkin ゲートを適用すればよい．

入力			出力		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	1
1	0	0	1	0	0
1	0	1	0	1	1
1	1	0	1	1	0
1	1	1	1	1	1

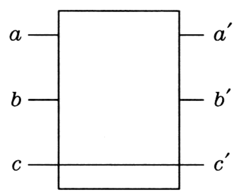


図 3.15: Fredkin ゲートの真理値表と回路表現．制御ビット c が 1 ならばビット a, b は交換され，0 ならばそのままに保たれる．

演習 3.29:（Fredkin ゲートの自己反転） Fredkin ゲートを 2 度継続して適用すると入力と同じ出力を与えることを示せ．

図 3.14 のビリヤードボールの経路を調べると，ビリヤードボール コンピュータが Fredkin ゲートを実現したものであることを証明するのは難しくない．

演習 3.30: 図 3.14 のビリヤードボール コンピュータが Fredkin ゲートを計算するものであることを証明せよ．

可逆性に加えて，Fredkin ゲートは入出力間で 1 の数が**保存** (conserve) されるという興味深い性質を持っている．ビリヤードボール コンピュータに当てはめると Fredkin ゲートに入る玉の数が出ていく数に等しいことに相当する．このため**保存的** (conservative) 可逆論理ゲートと呼ばれることがある．このような可逆性と保存性は基礎的物理原理に根差している可能性があるので，物理学者にとって興味深い．量子力学の測定公理は例外として，2.2.3 項で議論したように自然界の法則は可逆的である．この保存性は質量保存やエネルギー保存のような性質と類

似のものと考えられる．実際，ビリヤードボールの計算の保存性はまさに質量保存に対応している．

Fredkin ゲートは可逆的で保存的であるだけでなく，普遍的論理ゲートでもある！図 3.16 に示すように Fredkin ゲートは AND, NOT, CROSSOVER, FANOUT の機能をシミュレートするように配置することができて，カスケード接続をすることが可能であって，どんな古典回路でもシミュレートできる．

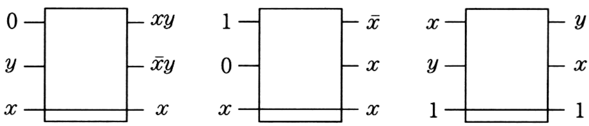


図 3.16: AND (左), NOT (中央) および単純な分配機能 CROSSOVER (右) の基本ゲートを実行するように配置された Fredkin ゲート．中央のゲートは x のコピーを 2 つ出力するので FANOUT 演算も実行できる．これらの配置では — 例えば AND ゲート第 1 入力の 0 のような — 標準状態の付加的な「補助」ビットを必要とすることと，出力に次の計算には不必要な「ごみ（不要データ）」が含まれることに注意．

AND のような非可逆ゲートを Fredkin ゲートでシミュレートするのに，我々は 2 つの概念を用いた．第 1 は Fredkin ゲート入力に特別の状態 0 または 1 の「補助」ビットを許容した．第 2 に Fredkin ゲート出力にその後の計算に用いられない無関係な「ごみ」(不要データ) を含ませた．重要なことはこれらがあるために計算が可逆になることである．実際 AND や OR などのゲートの非可逆性は補助ビットやごみビットが「隠れている」結果だと見なせる．まとめると，関数 $f(x)$ を計算するどんな古典回路が与えられても，入力 x と標準状態 a の補助ビットを用いて，$f(x)$ を計算し余分な「ごみ」出力 $g(x)$ を与えるような Fredkin ゲートだけからなる可逆回路を構築することができる．したがって，計算動作を $(x,a) \to (f(x), g(x))$ で表すことができる．

今や可逆的に関数を計算する方法がわかった．残念ながらこの計算法では望まないごみビットが生まれる．少し変形すると作られたすべてのごみビットが**標準状態** (standard state) になるような計算にすることができる．値が x に依存するごみビットは量子計算に重要な干渉性を破壊するので，この構成は量子計算にとって重要である．これがどのような働きをするかを理解するには，NOT ゲートが我々の可逆ゲートのレパートリーにあり，補助ビット a がすべて 0 から出発すると仮定すると役に立つ．補助ビットを 0 から 1 に変える必要があれば NOT ゲート

を付加する．また，古典的制御 NOT ゲートも利用できると仮定するとよい．古典的制御 NOT は 1.3.2 項の量子的定義と同様に定義され，入力 $(c,\ t)$ が $(c,\ t\oplus c)$ に変換される．ここで $\oplus$ は 2 を法とする和を表す．$t=0$ ならば $(c,\ 0)\to(c,\ c)$ なので，制御 NOT は可逆なコピーゲートあるいは FANOUT であると考えてよく，出力にごみビットを残さない．

回路の最初に NOT ゲートを追加すると計算の動作は $(x,\ 0)\to(f(x),\ g(x))$ と書ける．後に続く計算で変化しない x のコピーを作るために，回路の始めに制御 NOT ゲートも追加することもできるであろう．この変更をすれば回路の動作は次のように書ける．

$$(x,\ 0,\ 0)\to(x,\ f(x),\ g(x)). \tag{3.7}$$

式 (3.7) によれば，**逆計算** (uncomputation) と呼ばれるアイディアを使って，計算時間をあまり犠牲にせずにごみビットを取り除くことができるので，これは可逆回路の動作を表現する便利な方法である．このアイディアは次のようなものである．レジスタが 4 つあるコンピュータがあり，初期状態 $(x,\ 0,\ 0,\ y)$ にあるとする．第 2 レジスタは計算結果を記憶し，第 3 ビットは計算のための作業空間つまりごみビット $g(x)$ に使われる．第 4 レジスタの使い方はまもなく述べるが最初は任意の状態 y にあるとする．

前と同様に f を計算するのに可逆回路を適用すると，結果は状態 $(x,\ f(x),\ g(x),\ y)$ となる．次に制御 NOT を用いて結果 $f(x)$ をビット毎に第 4 レジスタに加えると，機械の状態は $(x,\ f(x),\ g(x),\ y\oplus f(x))$ になる．しかし，$f(x)$ の計算に用いた全ステップは可逆であり，第 4 レジスタには影響しなかったので，f の計算に用いた逆の回路を適用すると，状態 $(x,\ 0,\ 0,\ y\oplus f(x))$ になる．通常我々は関数計算の記述から補助ビット 0 を省略して回路動作を次のように書く．

$$(x,y)\to(x,y\oplus f(x)). \tag{3.8}$$

原理上 f を計算するのに用いられる可逆回路は他に多数存在するが，一般に f を計算するこの変形回路を f を計算する可逆回路と呼ぶ．

可逆計算を行う際に負担すべきリソースは何か？ この疑問を解析するには，可逆回路に必要な付加的な補助ビット数を勘定して，ゲート数を古典的モデルと比較する必要がある．可逆回路におけるゲート数は，次の種々の要素を表す一定の

因子の範囲内で，非可逆回路の場合に等しいことを明らかにしなければならない．その因子とは，非可逆回路中の1個の要素をシミュレートするに要するFredkinゲートの数，逆計算のための付加因子2，および回路中に含まれるビット数に比例する可逆計算に使われる付加的な制御NOT演算に対する負担分である．同様に非可逆回路中の各要素は一定数の補助ビットを用いてシミュレートできるので，必要な補助ビット数は非可逆回路中のゲート数とたかだか比例して変化する．その結果，可逆的あるいは非可逆的いずれの計算モデルを使っても，**P**や**NP**のような自然な計算量クラスは変わらない．**PSPACE**のような手の込んだ計算量クラスでは状況はそれほど直ちに明白ではない．そのような微妙な点については，問題3.9と「歴史と参考資料」を参照して欲しい．

演習 3.31:（可逆な半加算器） 2つのビットx, yが入力であるとき$(x,\ y,\ c,\ x\oplus y)$を出力とする可逆回路を構築せよ．ここでcはxとyが加えられたときの桁上げビットを表す．

Fredkinゲートとビリヤードボール コンピュータによる実現法は可逆計算の素晴らしいパラダイムを提供する．もう1つ別の可逆論理ゲートである**Toffoliゲート** (Toffoli gate) も古典計算に対する普遍的ゲートである．Toffoliゲートは Fredkinゲートに対するビリヤードボール構成のように，簡潔さと物理的単純さを持っているわけではないが，量子計算にはより有効である．1.4.1項ですでにToffoliゲートについて見たが，便宜上ここでその性質を概観する．

Toffoliゲートは3つの入力ビットa, b, cを有する．aとbを第1と第2の**制御ビット**，cを**標的ビット**と呼ぶ．このゲートでは2つの制御ビットは不変に保ち，両制御ビットが共に1であるときに標的ビットを反転させる．Toffoliゲートに対する真理値表と回路表現を図3.17に示す．

Toffoliゲートをどう使うと普遍的計算ができるのか？ ビットaとbのNANDをとるとする．Toffoliゲートを用いてこれを行うには，図3.18に示すように制御ビットとしてa, bを入力し，1に設定した補助ビットを標的ビットとする．aとbのNANDが標的ビットとしての出力である．Fredkinゲートから予想されるように，NANDのToffoliゲートシミュレーションには特別の補助ビット入力が必要であり，シミュレーション出力のうちのあるものはごみビットである．

Toffoliゲートは最初の制御ビットに補助ビット1，第2制御ビットにaを入力

入力			出力		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

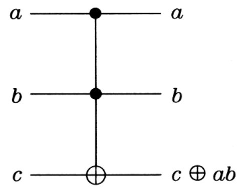


図 3.17: Toffoli ゲートの真理値表と回路表現.

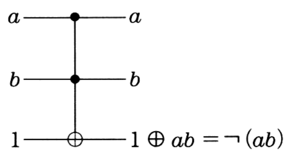


図 3.18: Toffoli ゲートを用いた NAND ゲート．上の 2 つのビットは NAND への入力，第 3 ビットは**補助状態**とも呼び，標準状態 1 に設定する．NAND 出力は第 3 ビットに現れる．

し，出力に 1, a, a を出すことにより FANOUT 演算を実行するにも使える．これを図 3.19 に示す．NAND と FANOUT は計算に普遍的であることを思い出すと，Toffoli ゲートと補助ビットだけからなる可逆回路を用いて任意の回路を効率良くシミュレートできること，および Fredkin ゲートで使ったように逆計算の便利なテクニックが使えることがわかる．

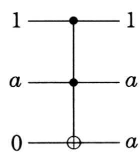


図 3.19: Toffoli ゲートを用いた FANOUT．第 2 ビットが FANOUT の入力で他の 2 つが標準補助状態．FANOUT の出力は第 2 と第 3 ビットに現れる．

可逆計算に対する我々の興味は，計算に要するエネルギーを理解したいという動機に基づいていた．雑音のないビリヤードボールの計算モデルを動作させるのに，エネルギーが要らないのは明らかである．Toffoli ゲートに基づくモデルではどうか？ これを決めるには Toffoli ゲート自体の計算モデルを調べなければなら

ない．7 章ではそのような幾つかの実現法について調べ，実際に Toffoli ゲートがエネルギーを消費せずに実行できることを知る．

エネルギーを消費することなく計算ができるという概念には重要な注意が必要である．前に述べたようにビリヤードボールの計算モデルは雑音に極めて敏感であり，これは可逆計算の他の多くのモデルにも当てはまる．雑音の影響を無くするには，何かの形の誤り訂正をする必要がある．通常そのような誤り訂正には，システムが予期通りの振る舞いをしているか，あるいは誤りが生じたかを決める測定をシステムに対して行う．コンピュータの記憶装置は有限なので，誤り訂正に使われる測定結果を記憶するために，新しい結果を記憶する余地を作るべく最後に使ったビットを消去する．Landauer の原理によれば，計算の全エネルギーコストの勘定に算入するべきエネルギーコストは，このビットの消去が担っている．誤り訂正に関連したエネルギーコストは 12.4.4（第 III 巻）で詳しく解析する．

可逆計算の研究から得られる結論は何か？ 鍵となる概念がが 3 つ含まれている．第 1 は可逆性は情報の各ビットを見失わないようにするのが基本である．情報が失われたり，消去されたときにのみ非可逆性が生じる．第 2 に計算を可逆的に行うことにより，計算中のエネルギー消費を無くすることができる．原理上エネルギーコストなしに全計算が行える．第 3 に計算入力に値が依存するごみビットの発生を抑えると，効率良く可逆的計算が行える．つまり，関数 f を計算する非可逆回路があると，$(x, y) \to (x, y \oplus f(x))$ の操作によりその回路を可逆回路で効率良くシミュレートできる．

物理学，コンピュータ科学，および量子計算と量子情報にとってこれらの結果は何を意味するか？ 物理学者やハードウェア技術者にとって良い知らせは，実際上システムの安定性と雑音の受けにくさの点からエネルギー消費が必要であるとはいえ，原理上計算を可逆的にすることによりエネルギー消費を無くすことができる．基本的レベルでは可逆計算を可能にする概念により，1 世紀前から物理学の基本であった有名な **Maxwell の悪魔** (Maxwell's demon) の問題も解けるようになる．この問題に関する経緯とその解についてはコラム 3.5 で紹介する．コンピュータ科学者の視点では，可逆計算による Turing 機械のような計算モデルによって，（それを使っても使わなくても多項式時間の同等なモデルになるので）非可逆的要素を使うことが正当化される．さらに物理的世界は基本的に可逆なので，可逆モデルに基づく計算量クラスは非可逆モデルに基づく計算量クラスより

自然である．この点は問題 3.9 と「歴史と参考資料」でもう一度触れる．量子計算と量子情報の観点から可逆計算は非常に重要である．量子計算の全能力を利用するには，量子計算における古典的サブルーチンを可逆的に，かつ古典的入力に依存するごみビットの発生なしに実行しなければならない．

演習 3.32:（Fredkin から Toffoli，Toffoli から Fredkin へ） Toffoli ゲートをシミュレートするに必要な最少の Fredkin ゲート数は幾つか？ Fredkin ゲートをシミュレートするに必要な最少の Toffoli ゲート数は幾つか？

補遺：本項には重要な補題 (lemma) が欠落している．本項では関数 $f(x)$ を計算する古典回路が与えられると，変換 $(x,\ y) \to (x,\ y \oplus f(x))$ を計算するために，同等に多くの可逆ゲートを用いて可逆回路を如何に作るかを説明している．（この証明は，出力が 0 か 1 かの単一ビットである関数に対して明示的に与えられているが，明らかに多重ビット出力に対しても成立する．このときには $\oplus$ をビット毎の 2 を法とする加法とする．）その補題を次に示す．

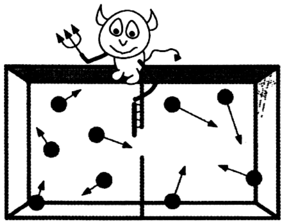
補題： もし $f(x)$ と $f^{-1}(x)$ が置換であって，**両方とも**多項式サイズの（多分可逆でない）古典回路を持つならば，補助ビット無しで $x \to f(x)$ を計算する多項式サイズの可逆回路が存在する．

この証明は既に紹介した可逆計算テクニックを用いて，$(x,0) \to (x, f(x)) \to (x \oplus f^{-1}(f(x)), f(x)) \to (0, f(x))$ を計算する．この結果は例えば Shor のアルゴリズムの章で暗に使われる．

コラム 3.5: Maxwell の悪魔

熱力学の法則は熱力学的平衡状態にある物理システムにより行われる仕事の量を支配する．この法則の 1 つである熱力学第 2 法則によれば，閉じたシステムの**エントロピー**は決して減少しない．1871 年に James Clerk Maxwell は一見この法則に反する機械が存在すると発表した．彼は下の図に描いたような小さな「悪魔」を想像した．その悪魔は速い分子と遅い分子を 1 つずつ 2 つの小部屋に分離することによって，最初熱平衡にあるガス容器のエントロピーを減少させることができる．この悪魔は小部屋間のドアに座って左か

ら速い分子が来るとドアを開けて分子を通し，その後ドアを閉じる．これを何度も繰り返すと容器の全エントロピーを**減少**させることができて，熱力学第2法則が破られる．



Maxwell の悪魔の逆説を解く鍵は，分子の速度を決定するのに悪魔は小部屋間を動く分子の**測定**を行わなければならない，という事実にある．この測定結果は悪魔の記憶装置に蓄積されねばならない．如何なる記憶装置も有限なので新しい結果を記憶する余地を作るために，悪魔は最終的には記憶から情報を消去しなければならない．Landauer の原理によれば情報を消去する動作により — 悪魔，ガス容器およびその環境という — 結合システムの全エントロピーが増加する．実際に完全な解析をすると，結合システムのエントロピーは情報を消去する動作によって，悪魔の動作による減少分と**少なくとも同じだけ**増加する．この結果熱力学第2法則が成り立つことが保証される．

3.3 コンピュータ科学の展望

本章のような短い紹介では豊かなコンピュータ科学分野における，偉大な概念をすべて詳細にカバーすることはおよそ不可能である．コンピュータ科学者のように**考える**ことが何を意味するかを読者に伝え，計算を理解する際に重要な基本的概念の用語とあらましが提供できたと思う．本章を終えるに当たり，コンピュータ科学の全貌の中で量子計算と量子情報が占める見通しを得るために，一般的な事項に触れておく．

我々は Turing 機械を中心に議論を展開した．大規模並列処理, DNA コンピュータ，アナログコンピュータのような，非伝統的な計算モデルの計算能力は標準的

な Turing 機械計算モデルと比較してどうなのか？ そして間接的に量子計算と比較してどうなのか？ 並列計算アーキテクチャから考える．現在存在するほとんど大部分のコンピュータは，中央処理装置で一時に1つの命令を実行する直列的なコンピュータである．これに対して並列コンピュータでは一時に1つ以上の命令を処理することができ，ある種の応用には時間と費用を十分に節約することができる．それにもかかわらず効率性に関する限り，並列処理は標準的 Turing 機械に比べて基本的な長所を持っていない．その理由は Turing 機械は多項式的に等価な全物理的リソース — 計算に必要な空間と時間 — で並列コンピュータをシミュレートできるからである．並列計算が時間で得をするときには，計算に要する全空間的リソースの点で損をするので，結果として計算モデルの能力は本質的な違いがない．

大規模並列計算の興味ある例に **DNA 計算** (DNA computing) というテクニックがある．1本の DNA つまりデオキシリボ核酸は A (アデニン), C (シトシン), G (グアニン), T (チミン) という文字で表す塩基により区別される4種の核酸の配列（高分子）で構成される分子である．塩基対（A と T，G と C）が互いに相補って，ある状況下で2本の鎖がアニールされて2重鎖が形成される．両端も互いに異なっていて適切に相補うものになっている．化学のテクニックを用いて特定配列の始端または終端を持つ鎖の数を増やし（ポリメラーゼ連鎖反応），長さ毎に鎖を分離し（ゲル電気泳動），2重鎖を1重鎖に分解し（温度と pH の変化), 鎖上の塩基配列を解読し，特定場所で鎖を切断し（制限酵素），そして試験管中で DNA のある配列ができたかどうかを検出する．これらの荒っぽい機構を用いた手続きは複雑であるが，基本となる考え方は次の例から評価できる．

Hamilton 有向路問題は単純であるが，3.2.1 項で述べた Hamilton の閉路問題の変形であって，同じように困難な問題である．N 個の頂点を持つ有向グラフ G において各頂点に厳密に1度だけ入り，辺を許された方向にたどって2つの特定の頂点 j_1 と j_N の間に路が存在するか否かを決めるのが目的である．この問題は DNA コンピュータを用いて次のステップで解くことができる．x_j を一意の塩基配列（を $\bar{x}_j$ をその補足配列）となるように選び，鎖 x_jx_k で辺を符号化し，鎖 $\bar{x}_j\bar{x}_j$ で頂点を符号化する．

(1) すべての可能な頂点と辺の DNA 鎖の混合物を組み合わせて，鎖がアニールするまで待って G を通るランダムな路を生成する．

(2) $\bar{x}_{j_1}$ から始まり $\bar{x}_{j_N}$ に終わる 2 重鎖だけを増幅して，j_1 から始まり j_N に終わる路だけを残す．

(3) 長さに応じて鎖を分離して，長さ N の路だけを選び出す．

(4) DNA を 1 重鎖に分解した後，一時に 1 つずつすべての可能な頂点鎖をアニールし，アニールした鎖だけを濾過して取り出すことにより，各頂点に少なくとも 1 回入る路だけを選び出す．

(5) この選別段階を通過した鎖を検出して，もしあれば路が存在し，なければ存在しない．

十分高い確率で答えが正しいと保証するために，x_j は多数（≈ 30）の塩基を含むように選び，反応には多数（$\approx 10^{14}$）の DNA 鎖が用いられる．

この基本概念を改善するのに発見的方法が用いられる．もちろんこのような絨毯爆撃的方法が有効なのはすべての路が効率良く生成される場合に限られ，分子の数は問題のサイズ（上の例では頂点数）と共に指数関数的に増加する．DNA 分子は比較的小さく容易に合成できて，DNA の組み合わせの膨大な数を試験管中に収められるので，しばらくは — 頂点の数が数十までは — 指数関数的な計算量コストの増加を食い止めることができるが，究極的には指数関数的コストによってこの方法の適用性が制限される．したがって，DNA 計算がある種の問題を解くために物理的に実現可能で魅力的な計算モデルを提供する一方，それは古典計算テクニックであって Turing 機械を越える本質的改善を提供するものではない．

アナログコンピュータ (analogue computer) はもう 1 つ別の計算パラダイムを提供する．アナログコンピュータで計算に使う情報は 0 と 1 でなく連続な自由度を持つ．例えば温度計はアナログコンピュータである．抵抗，静電容量，増幅器を用いたアナログ回路もアナログ計算を行うといえる．位置とか電圧のような連続変数は無制限の情報量を記憶するので，理想的極限でこの機械は無限のリソースを使う．しかしこれは雑音がない場合の話であって，有限量の雑音があると連続変数の**識別可能な状態**の数は有限数に減少する．この結果，アナログコンピュータは有限情報の表現に制約される．実際雑音によってアナログコンピュータの能力は通常のディジタルコンピュータ以下，したがって Turing 機械以下に減退する．量子コンピュータも q ビット状態を記述するのに連続パラメータを使うので，単なるアナログコンピュータであると疑う向きがあるかも知れない．しかし，量

子コンピュータ上の雑音の効果は実効的に**ディジタル化**されることがわかっている．その結果有限量の雑音が存在しても量子コンピュータの計算上の優位性は変わらない．この点は10章（第III巻）で議論する．

ディジタルコンピュータへの雑音の影響はどうか？計算の初期時代に雑音は本当に大問題であった．初期のコンピュータでは真空管は数分ごとに誤動作を繰り返した．今日でもモデムやハードディスクのようなコンピュータデバイスにとって雑音は問題である．信頼度の高くない部品を使って信頼度の高いコンピュータを如何に構築するか，を理解するのにかなりの努力がなされた．計算時に多項式時間のリソース増加を来すだけで，これが可能であることがvon Neumannによって証明された．しかし，皮肉にも現在の部品は信頼性が素晴らしく高いので，現代のコンピュータはこの結果を利用していない．現在の電子部品の故障率は10^{-17}以下なので故障は稀にしか起きず，それを防ぐ余計な努力をする意味がないと考えられている．他方で量子コンピュータは非常に繊細な機械であり，誤り訂正のテクニックを適用する必要がありそうである．

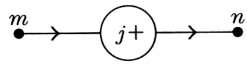
アーキテクチャが変化すると雑音の影響も変わる．例えば，もし雑音の影響が無視できれば，多くの演算を並列に行うアーキテクチャに変えても，実行すべき演算数は変わらない．しかし，並列システムは雑音の効果が蓄積しにくいので本質的に雑音に強い．したがって，実際の解析では，並列版アルゴリズムが直列版より本当に利点がある．古典コンピュータのアーキテクチャ設計は十分進歩した研究分野である．量子コンピュータで同様のものはほとんど開発されていないが，雑音の研究によれば将来の量子コンピュータに対して高度の並列性のような望ましい特色がすでに示唆されている．

第4の計算モデルは空間的に離れた2つ以上の計算ユニットが計算問題に使用される**分散計算** (distributed computation) である．明らかにこの計算モデルは，Turing機械上で効率良くシミュレートできるという意味で，Turing機械より強力ではない．しかし，分散計算はユニット間の**通信コスト**が高いときに多数の計算ユニットを如何にうまく利用するか？という，新たなリソースへの挑戦プランを提起する．この分散計算の問題はコンピュータ間が高速ネットワークでつながれているときに特に興味深い．ネットワーク上の全コンピュータの全計算容量は非常に大きいけれども，その能力を使うことは難しい．最も興味ある問題では，容易く小分けにして独立なかたまりを別々に解くことができず，異なる計算サブシ

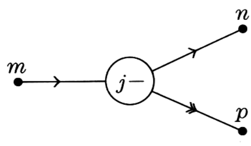
ステム間で中間結果の交換や内部状態の同期のための包括的な通信を頻繁に必要とする．このような問題を扱うために**通信量** (communication complexity) の分野が研究され，問題を解く際の通信コストの要求を定量化している．量子リソースが利用できて分散コンピュータ間で交換されれば通信コストは大いに減少できる場合があろう．

ここでの結論と本書全体を通じて繰り返し出てくるテーマは，これまでコンピュータ科学は物理的制約から独立であったにもかかわらず，コンピュータをどう実現するかだけでなく，解ける問題のクラスにまで究極的に物理法則が途方もなく大きなインパクトを与えることである．物理学的に合理的なもう 1 つの計算モデルとしての量子計算と量子情報の成功は，コンピュータ科学の堅い信念に疑問を抱き，コンピュータ科学の概念を物理学の最前線に押し進める．本書ではこれからこれら異なる分野の考えを組み合わせて，その結果に期待することとする．

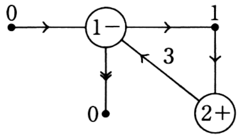
問題 3.1:（Minsky の機械）　Minsky の機械 (Minsky machine) は任意の負でない整数を記憶できる有限個の**レジスタ** (register) r_1，$r_2, \ldots, r_k$ と，2 つのタイプ内の 1 つの**指令** (order) で作られる**プログラム** (program) により構成される．第 1 のタイプは次の形を有する：



この解釈はプログラムの点 m で実行するとレジスタ r_j が 1 だけ増加して，プログラムの点 n に進む．第 2 の指令のタイプは次の形である：



この解釈はプログラムの点 m で実行するとレジスタ r_j の内容が正の整数ならば減算してプログラムが点 n に進み，内容が 0 ならば単にプログラムの点 p に進む．Minsky 機械の**プログラム**はこれら指令の集まりでできており次のような形をしている：



プログラムに対する出発点と可能な停止点は 0 の記号で表すのが慣用である．このプログラムではレジスタ r_1 の内容を取ってレジスタ r_2 に加え，r_1 を 0 にする．

(1) 計算可能な関数 $f(\cdot)$ が与えられたときに，レジスタが $(n,\ 0,\dots,0)$ から出発して，出力 $(f(n),\ 0,\dots,0)$ を与える Minsky 機械が存在するという意味で，すべての (Turing 機械で) 計算可能な関数は Minsky 機械で計算できることを示せ．

(2) 上記の意味で Minsky 機械により計算可能な任意の関数は Turing 機械でも計算できる証明の概略を述べよ．

問題 3.2: **(ベクトルゲーム)**　**ベクトルゲーム** (vector game) は同一次元で整数座標を有するベクトルの有限個のリストで規定される．ゲームは負でない整数座標のベクトル x から出発して，この x に加えても全成分が負でないという性質を保存するリスト中のベクトルの最初のものを加え，これができなくなるまで繰り返す．任意の計算可能な関数 $f(\cdot)$ に対して，ベクトル $(n,\ 0,\dots,0)$ から出発して $(f(n),\ 0,\dots,0)$ に到達するベクトルゲームが存在することを証明せよ．(ヒント：$k+2$ 次元のベクトルゲームが k 個のレジスタを含む Minsky 機械をシミュレートできることを示せ．)

問題 3.3: **(Fractran)**　**Fractran プログラム** (Fractran pgrogram) は正の有理数リスト $q_1,\dots,q_n$ で定義される．このプログラムは正の整数 m に働いてこれを $q_i m$ に置き換える．ここで i は $q_i m$ が整数になるような最小の数である．もし $q_i m$ が整数になるような i が存在しなくなると計算が停止する．任意の計算可能な関数 $f(\cdot)$ に対して 2^n から出発したときに，途中の 2 のベキの値を通ることなく $2^{f(n)}$ に達するような Fractran プログラムが存在することを証明せよ．(ヒント：前の問題を使え．)

問題 3.4: **(ダイナミックシステムの非決定性)**　Fractran プログラムの本質は，正の整数を正の整数に対応させる非常に単純なダイナミックなシステムで

ある．そのようなダイナミックシステムが 1 に到達するかどうかを決定するアルゴリズムはないことを証明せよ．

問題 3.5:（2 ビット可逆論理の非普遍性） 1 ないし 2 ビットの可逆論理ゲートと補助ビットだけを使って回路を構築するとする．この方法で計算できない Boole 関数が存在することを証明せよ．Toffoli ゲートは補助ビットを使っても，1 ビットと 2 ビットの可逆ゲートを使ってシミュレートできないことを導け．

問題 3.6:（TSP 近似の困難さ） $r \geq 1$ として倍数 r の範囲内で，n 都市間を巡る最短経路を見付けることを保証する TSP の近似アルゴリズムが存在するとする．$G = (V,\ E)$ は n 個の頂点上の任意のグラフとする．頂点 V を都市と見なし，$(i,\ j)$ が G の辺ならば都市 i と j の都市間の距離を 1 とし，そうでなければ $\lceil r \rceil |V| + 1$ として，TSP の事例を定義する．この TSP の事例に近似アルゴリズムを適用するとき，もし存在するならば Hamilton の閉路を返し，存在しないならば $\lceil r \rceil |V|$ 以上の通路長を返すことを示せ．HC が **NP** 完全であることから，$\mathbf{P} = \mathbf{NP}$ でなければそのような近似アルゴリズムは存在し得ない．

問題 3.7:（可逆 Turing 機械）

(1) 通常の Turing 機械上で計算できるのと同じクラスの関数を計算できる，可逆的 Turing 機械の構築法を説明せよ．（ヒント：多テープ構成を用いるとよいかも知れない．）

(2) この可逆 Turing 機械の動作に対する一般的な空間と時間の限界を，通常の単一テープ Turing 機械が関数 $f(x)$ を計算するに要する時間 $t(x)$ と空間 $s(x)$ を用いて表せ．

問題 3.8:（関数の計算困難なクラスを見出す（研究）） 計算するのに超多項式数 (super-polynomial) の Boole ゲートを必要とする，n 入力の関数の自然なクラスを見出せ．

問題 3.9:（可逆 PSPACE = PSPACE） 「定量化充足可能性問題」(quantified satisfiability problem) つまり QSAT 問題は **PSPACE** 完全である

ことが示せる．すなわち，**PSPACE** の他の全言語は多項式時間で QSAT に縮約できる．言語 QSAT は n 個の変数 $x_1, \ldots, x_n$ で論理積標準形の全 Boole 関数 φ よりなるとして，次のように定義される：

$$\exists_{x_1}\forall_{x_2}\exists_{x_3}\ldots\forall_{x_n}\ \varphi;\ n\text{ が偶数のとき,} \tag{3.9}$$

$$\exists_{x_1}\forall_{x_2}\exists_{x_3}\ldots\exists_{x_n}\ \varphi;\ n\text{ が奇数のとき.} \tag{3.10}$$

多項式空間で動作する可逆 Turing 機械を用いて，QSAT を解くことができるのを証明せよ．したがって，多項式空間で可逆的に働くコンピュータで決定できる言語のクラスは **PSPACE** に等しい．

問題 3.10:（補助ビットと可逆計算の効率） p_m は m 番目の素数とする．$n > m$ を満たす入力 m, n に対して積 $p_m p_n$ を出力する可逆回路，つまり $(m, n) \to (p_m p_n,\ g(m, n))$ の可逆回路を構成する概略を示せ．ここで $g(m, n)$ は回路に使われる補助ビットの最終状態である．その回路が必要とする補助 q ビットの数を推定せよ．もし $O(\log(\log n))$ 個の補助ビットを用いる（$\log n$ の）多項式サイズの可逆回路が見付かれば，2 つの素数の積を因数分解する問題は **P** にあることを証明せよ．

歴史と参考資料

コンピュータ科学は多くの興味ある分野を含む巨大な主題である．この短いスペースでは完全を期すことはとてもできないが，読者が興味を持つことを期待して，この機会に一般的に興味のある二三の書籍や本書で扱う話題に関係した著作を推薦する．

現代のコンピュータ科学は Turing の素晴らしい 1936 年の論文 [Tur36] にさかのぼる．Church-Turing の提唱は Church により 1936 年に述べられ [Chu36]，その後 Turing によって異なる観点からより完全に議論された．ほぼ同時期に数人の研究者がそれぞれの方法で同じ結論を導いた．これら貢献の多くとその歴史に関する議論は Davis が編集した書物 [Dav65] に見られる．Church-Turing の提唱と非決定性の刺激的議論が Hofstadter [Hof79] と Penrose [Pen89] に見られる．

アルゴリズム設計には優れた本が多い．3 つだけ紹介する．最初は Knuth の古

典的シリーズ [Knu97] [Knu98a] [Knu98b] であり，コンピュータ科学の膨大な部分を網羅している．第 2 には，Cormen, Leiserson, Rivest による素晴らしい著作がある [CLR90]．この膨大な本にはアルゴリズム設計の多くの領域についての材料が豊富に掲載されている．最後に Motwani と Raghaven の書物 [MR95] は確率的アルゴリズム分野の優れた概論である．

近代的計算量理論は Cook [Coo71] と Karp [Kar72] の論文に特に影響を受けた．多くの同様のアイディアが Levin[Lev73] によりロシアで提出されたが，不幸にして西欧に伝わるのに時間がかかった．Garey と Johnson の古典的な本 [GJ79] もこの分野に大きな影響を与えた．より最近では Papadimitriou は計算量理論の多くの主要概念を見渡した美しい本 [Pap94] を出版した．本章の多くの材料は Papadimitriou の書物に基づいている．本章では言語間の可約性について多項式時間の縮約しか考えなかった．他にも言語間の縮約には多くの考えが存在する．初期のこれらの概念は Ladner，Lynch，Selman の解説 [LLS75] がある．異なる縮約概念の研究はその後**構造的複雑性** (structural complexity) と呼ばれる研究分野へと開花し，Balcázar, Diaz, Gabarró [BDG88a] [BDG88b] が解説している．

情報，エネルギー消費と計算の間の関係には長い歴史がある．現代の理解は Landauer による 1961 年の論文 [Lan61] に基づいており，そこで Landauer の原理が最初に定式化された．Szilard [Szi29] と von Neumann の 1949 年の講義 [von66] も Laudauer の原理に近い結論に到達しているが，散逸を必要とするのは情報の**消去** (erasure) であるという本質的な点を十分に捕捉していない．

可逆な Turing 機械は Lecerf [Lec63] により発明され，その後独立に Bennett の影響力のある論文 [Ben73] で述べられている．Fredkin と Toffoli [FT82] は計算の可逆回路モデルを導入した．Barton の 1978 年 5 月の MIT 6.895 学期報告 [Bar78] と Ressler の修士論文 [Res81] は 2 つの興味深い歴史的論文であり可逆 PDP-10!の設計が掲載されている．今日可逆論理は低電力 CMOS 回路 [YK95] の実現に潜在的に重要である．

Maxwell の悪魔は興味深い話題であり，長く難解な歴史を持っている．Maxwell は 1871 年に彼の悪魔を提唱した [Max71]．Szilard は 1929 年に重要な論文を発表し [Szi29]，Maxwell の悪魔の問題を最終的に解くための詳細を予測した．1965 年に Feynman [FLS65b] は Maxwell の悪魔の特別な場合を解決した．Bennett は Laudauer の論文 [Lan61] を基にこの問題に関して 2 つの素晴らしい論文 [Ben82]

[Ben87] を執筆して，この問題の解を完成した．Maxwell の悪魔とその悪魔払いに関する歴史は Leff と Rex による論文集 [LR90] が興味深い．

DNA 計算は Adleman により発明され，ここに述べた Hamilton の有向路問題の解は彼によるものである [Adl94]．Lipton もこのモデルで 3SAT と回路充足可能性問題が解けることを示した [Lip95]．一般向けの優れた論文は Adleman の Scientific American の論文 [Adl98] である．DNA 演算の普遍性に関する洞察力に富む論文は Winfree [Win98] を参照して欲しい．雑音があるときの信頼度の高い計算処理について知りたければ Wingrad と Cown[WC67] が興味深い．この話題については 10 章（第 III 巻）でもう一度述べる．コンピュータのアーキテクチャに関する良い教科書には Hennessey, Goldberg, Patterson [HGP96] がある．

問題 3.1 から 3.4 は Minsky（彼の計算機械に関する素晴らしい書物 [Min67]）が創始し，Conway[Con72][Con86] が発展させた一連の思考を追求している．Fractran プログラム言語は確かに知る限りで最も美しく簡潔な普遍的計算モデルであり，PRIMEGAME と呼ばれる次の例で実証された [Con86]．PRIMEGAME は有理数のリストで定義される：

$$\frac{17}{91};\ \frac{78}{85};\ \frac{19}{51};\ \frac{23}{38};\ \frac{29}{33};\ \frac{77}{29};\ \frac{95}{23};\ \frac{77}{19};\ \frac{1}{17};\ \frac{11}{13};\ \frac{13}{11};\ \frac{15}{2};\ \frac{1}{7};\ \frac{55}{1}. \quad (3.11)$$

驚くべきことに PRIMEGAME が 2 から出発すると現れる他のベキ乗は，素数を順に 1 つずつ昇るベキを持つ正確に 2 の素数乗 2^2, 2^3, 2^5, 2^7, 2^{11}, 2^{13}, ... になる．問題 3.9 は可逆計算への空間的要請に関する一般的トピックスの特別な場合に当たる．Bennett [Ben89] と Li, Tromp, Vitanyi [LV96] [LTV98] の論文を参照されたい．

付録A　確率論の基礎

この付録には確率論に関する基本的な定義と結果を集めてある．読者は既にこの分野に関してなにがしかの知識を持っていることを仮定している．これらの結果に精通していない読者は，演習で示されているようにこの内容を時間をとって証明したほうがよい．

確率論の基本的概念は**確率変数** (random variable) である．確率変数 X は確率 $p(X = x)$ で値の 1 つ x をとる．確率変数を表すのに大文字 X，確率変数がとる値を表すのに小文字 x を用いる．「$X =$」を隠して $p(X = x)$ の代わりに記号 $p(x)$ をよく使う．本書では常に有限集合の値をとる確率変数だけを扱うと仮定する．時によっては，例えば集合 (i, j)，$i = 1, \ldots, m_1$，$j = 1, \ldots, m_2$ の値をとるベクトルを値に持つ確率変数を考えるのが便利なことがある．

もし $X = x$ が与えられたときに $Y = y$ となる確率，つまり**条件付き確率** (conditional probability) は次式で定義される：

$$p(Y = y|X = x) \equiv \frac{p(X = x,\ Y = y)}{p(X = x)}, \tag{A.1}$$

ここで $p(X = x,\ Y = y)$ は $X = x$ **および** $Y = y$ である確率である．$p(X = x) = 0$ ならば $p(Y = y|X = x) = 0$ と約束する．「$Y =$」と「$X =$」を隠して $p(y|x)$ という記号をよく使う．もしすべての x, y に対して $p(X = x,\ Y = y) = p(X = x)p(Y = y)$ ならば，X と Y は**独立** (independent) であるという．X と Y が独立であるとき，すべての x と y に対して $p(y|x) = p(y)$ である．

Bayes の規則 (Bayes' rule) は X が与えられたときの Y の条件付き確率と

Y が与えられたときの X の条件付き確率との関係を示す：

$$p(x|y) = p(y|x)\frac{p(x)}{p(y)}. \tag{A.2}$$

この式に現れる確率 $p(y)$ は，次に議論する全確率の法則を用いて書き換えられることがある．

演習 A.1: Bayes の規則を証明せよ．

確率論において最も重要で頻繁に使われる結果は**全確率の法則** (law of total probability) である．その内容はもし X と Y が 2 つの確率変数ならば，Y に対する確率は X に対する確率と X が与えられたときの Y に対する条件付き確率で表現される：

$$p(y) = \sum_x p(y|x)p(x), \tag{A.3}$$

ここで総和は X がとり得るすべての x の値に対して行う．

演習 A.2: 全確率の法則を証明せよ．

確率変数 X の**期待値** (expectation) あるいは**平均値** (average, mean) は次式で定義される：

$$\mathbf{E}(X) \equiv \sum_x p(x)x, \tag{A.4}$$

ここで総和は確率変数 X がとり得るすべての値 x に関して行う．

演習 A.3: $p(x) > 0$ を満たす値 $x \geq \mathbf{E}(X)$ が存在することを証明せよ．

演習 A.4: $\mathbf{E}(X)$ は X に対して線形であることを証明せよ．

演習 A.5: 独立な確率変数 X, Y に対して $\mathbf{E}(XY) = \mathbf{E}(X)\mathbf{E}(Y)$ を証明せよ．

確率変数 X の**分散**(variance) は次式で定義される：

$$\mathrm{var}(X) \equiv \mathbf{E}[(X - \mathbf{E}(X))^2] = \mathbf{E}(X^2) - \mathbf{E}(X)^2. \tag{A.5}$$

標準偏差 (standard deviation) $\Delta(X) \equiv \sqrt{\mathrm{var}(X)}$ は，確率変数の散らばりを表す尺度である．**Chebyshev の不等式** (Chebyshev's inequality) は，標準偏差がどのような意味で確率変数の値の散らばりの尺度になるかを，より正確に表す．その表現するところは任意の $\lambda > 0$ と有限な分散を持つ確率変数 X に対して

$$p\big(|X - \mathbf{E}(X)| \geq \lambda\Delta(X)\big) \ \leq \frac{1}{\lambda^2}. \tag{A.6}$$

したがって，平均値より標準偏差の λ 倍以上離れている確率は λ が無限大になると小さくなる．

演習 A.6: Chebyshev の不等式を証明せよ．

本文ではこの他に Chernoff の限界（コラム 3.4)，Fano の不等式（コラム 12.2)，大数の法則（コラム 12.3）など，確率論の多くの結果が使われている．

歴史と参考文献

確率論には優れた教科書が氾濫している．特に確率 (probability) と確率過程 (stochastic process) の多くの基本概念に関する優れた入門書である Grimmett と Stirzaker [GS92] の教科書を推薦する．もっと純粋数学的観点からは Williams [Wil91] は近代確率論の素晴らしい入門書であり，マルチンゲール (martingale) の簡潔な理論が強調されている．最後に古典的な Feller [Fel68a] [Fel68b] の 2 巻の教科書は確率論の概念を詳細に紹介した優れた書である．

参考文献

[注 1] 第 I 部〜第 III 部（第 I 巻〜第 III 巻）全体に関する参考文献を示す.

[注 2] *arXive e-print quant-ph/xxxxxxx* の文献は http://www.arXiv.org のインターネットサイトから入手できる.

[ABO97] D. Aharonov and M. Ben-Or. Fault tolerant computation with constant error. In *Proceedings of the Twenty-Ninth Annual ACM Symposium on the Theory of Computing,* pages 176-188, 1997.

[ABO99] D. Aharonov and M. Ben-Or. Fault-tolerant quantum computation with constant error rate. *SIAM J. Comp.*, page to appear, 1999. *arXive e-print quant-ph/9906129.*

[ABOIN96] D. Aharonov, M. Ben-Or, R. Impagliazzo, and N. Nisan. Limitations of noisy reversible computation. *arXive e-print quant-ph/9611028*, 1996.

[ADH97] L. Adleman, J. Demarrais, and M. A. Huang. Quantum computability. *SIAM J. Comp.*, 26(5): 1524-1540, 1997.

[Adl94] L. M. Adleman. Molecular computation of solutions to combinatorial problems. *Science,* 266: 1021, 1994.

[Adl98] L. M. Adleman. Computing with DNA. *Sci. Am.*, 279: 54-61, Aug. 1998.

[AE75] L. Allen and J. H. Eberly. *Optical Resonance and Two-level Atoms.* Dover, New York, 1975.

[Aha99a] D. Aharonov. *Noisy Quantum Computation.* Ph.D. thesis, The Hebrew Univesity, Jerusalem, 1999.

[Aha99b] D. Aharonov. Quantum computation. In D. Stauffer, editor, *Annual Reviews of Computational Physics VI.* World Scientific, Singapore, 1999.

[AKN98] D. Aharonov, A. Kitaev, and N. Nisan. Quantum circuits with mixed states. *STOC 1997,* 1998. *arXive e-print quant-ph/9806029.*

[AL70] H. Araki and E. H. Lieb. Entropy inequalities. *Comm. Math. Phys.*, 18: 160-170, 1970.

[AL97] D. S. Abrams and S. Lloyd. Simulation of many-body Fermi systems on a quantum computer. *Phys. Rev. Lett.*, 79(13): 2586-2589, 1997. *arXive e-print quant-ph/9703054.*

[AL99] A. Ashikhmin and S. Lytsin. Upper bounds on the size of quantum codes. *IEEE Trans. Inf. Theory*, 45(4): 1206-1215, 1999.

[Alb83] P. M. Alberti. A note on the transition-probability over c-* algebras. *Lett. in Math. Phys.*, 7(1): 25-32, 1983.

[Amb00] A. Ambainis. Quantum lower bounds by quantum arguments. *arXive e-print quant-ph/0002066,* 2000.

[And79] T. Ando. Concavity of certain maps on positive definite matrices and applications to Hadamard products. *Linear Algebra Appl.*, 26: 203-241, 1979.

[Ash97] A. Ashikhmin. Remarks on bounds for quantum codes. *arXive e-print quant-ph/9705037,* 1997.

[Bar79] E. Barton. A reversible computer using conservative logic. Unpublished MIT 6.895 term paper, 1978.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing,* pages 175-179, IEEE, New York, 1984. Bangalore, India, December 1984.

[BBB+92] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin. Experimental quantum cryptography. *J. Cryptology,* 5: 3-28, 1992.

[BBB+98] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. Security of quantum key distribution against all collective attacks. *arXive e-print quant-ph/9801022,* 1998.

[BBBV97] C. H. Bennett, E. Bernstein, G. Brassard, and U. Vazirani. Strengths and weaknesses of quantum computing. *SIAM J. Comput.*, 26(5): 1510-1523, 1997. *arXive e-print quant-ph/9701001* .

[BBC+93] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and EPR channels. *Phys. Rev. Lett.*, 70: 1895-1899, 1993.

[BBC+95] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Phys. Rev. A,* 52: 3457-3467, 1995. *arXive e-print quant-ph/9503016.*

[BBC+98] R. Beals, H. Buhrman, R. Cleve, M. Mosca, and R. de Wolf. Quantum lower bounds by polynomials. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science (FOCS'98)* , pages 352-361, IEEE, Los Alamitos, California, November 1998. *arXive e-print quant-ph/9802049.*

[BBCM95] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory* 41: 1915-1923, 1995.

[BBE92] C. H. Bennett, G. Brassard, and A. K. Ekert. Quantum cryptography. *Sci. Am.*, 267(4): 50, Oct. 1992.

[BBHT98] M. Boyer, G. Brassard. P. Høyer, and A. Tapp. Tight bounds on quantum searching. *Fortsch. Phys. - Prog. Phys.,* 46(4-5): 493-505, 1998.

[BBM+98] D. Boschi, S. Branca, F. D. Martini, L. Hardy, and S. Popescu. Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolski-Rosen channels. *Phys. Rev. Lett.,* 80: 1121-1125, 1998. *arXive e-print quant-ph/9710013.*

[BBP+96] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.,* 76: 722, 1996. *arXive e-print quant-ph/9511027*

[BBPS96] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher. Concentrating partial entanglemeny by local operations. *Phys. Rev. A,* 53(4): 2046-2052, 1996. *arXive e-print quant-ph/9511030.*

[BBR88] C. H. Bennett, G. Brassard, and J. M. Robert. Privacy amplification by public discussion. *SIAM J. Comp.,* 17: 210-229, 1988.

[BCDP96] D. Beckman, A. N. Chari, S. Devabhaktuni, and J. Preskill. Efficient networks for quantum factoring. *Phys. Rev. A*, 54(2): 1034, 1996. *arXive e-print quant-ph/9602016.*

[BCF+96] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.,* 76(15): 2818-2821, 1996. *arXive e-print quant-ph/9511010.*

[BCJ+99] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.,* 83(5): 1054-1057, 1999.

[BCJD99] G. K. Brennen, C. M. Caves, P. S. Jessen, and I. H. Deutsch. Quantum logic gates in optical lattices. *Phys. Rev. Lett.,* 82: 1060-1063, 1999.

[BD00] C. H. Bennett and D. P. DiVincenzo. Quantum information and computation. *Nature,* 404: 247-55, 2000.

[BDG88a] J. L. Balcázar, J. Diaz, and J. Gabarró . *Structural Conrplexity,* Volume I. Springer-Verlag, Berlin, 1988.

[BDG88b] J. L. Balcázar, J. Diaz, and J. Gabarró . *Structural Complexity,* Volume II. Springer-Verlag, Berlin, 1988.

[BDK92] R. G. Brewer, R. G. DeVoe, and R. Kallenbach. Planar ion microtraps. *Phys. Rev. A,* 46(11): R6781-4, 1992

[BDS97] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin. Capacities of quantum erasure channels. *Phys. Rev. Lett.,* 78(16): 3217-3220, 1997. *arXive e-print quant-ph/9701015* .

[BDSW96] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed state entanglement and quantum error correction. *Phys. Rev. A,* 54: 3824, 1996. *arXive e-print quant-ph/9604024.*

[Bel64] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1: 195-200, 1964. Reprinted in J. S. Bell, *Speakable and Unspeakable in Quantum Mechanics*, Cambridge University Press, Cambridge, 1987.

[Ben73] C. H. Bennett. Logical reversibility of computation. *IBM J. Res. Dev.,* 17(6): 525-32, 1973.

[Ben80] P. Benioff. The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines. *J. Stat. Phys.,* 22(5): 567-591, 1980.

[Ben82] C. H. Bennett. The thermodynamics of computation — a review. *Int. J. Theor. Phys.,* 21: 905-40, 1982.

[Ben87] C. H. Bennett. Demons, engines and the second law. *Sci. Am.*, 295(5): 108, 1987.

[Ben89] C. H. Bennett. Time-space trade-offs for reversible computation. *SIAM J. Comput.,* 18: 766-776, 1989.

[Ben92] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.,* 68(21): 3121-3124, 1992.

[Bet84] T. Beth. *Methoden der Schnellen Fouriertransformation.* Teubner, Leipzig, 1984.

[BFGL98] S. L. Braunstein, C. A. Fuchs, D. Gottesman, and H. Lo. A quantum analog of Huffman coding. *arXive e-print quant-ph/9805080,* 1998.

[BFJS96] H. Barnum, C. A. Fuchs, R. Jozsa, and B. Schumacher. General fidelity limit for Quantum channels. *Phys. Rev. A,* 54: 707, 1996. *arXive e-print quant-ph/9603014.*

[Bha97] R. Bhatia. *Matrix Analysis.* Springer-Verlag, New York, 1997.

[BHT98] G. Brassard, P. Hayer, and A. Tapp. Quantum counting. *arXive e-print quant-ph/9805082,* 1998.

[BK92] V. B. Braginsky and F. Y. Khahili. *Quantum Measurement.* Cambridge University Press, Cambridge, 1992.

[BK98a] S. L. Braunstein and H. J. Kimble. Teleportion of continuous quantum variables. *Phys. Rev. Lett.,* 80: 869-72, 1998.

[BK98b] S. B. Bravyi and A. Y. Kitaev. Quantum codes on a lattice with boundary. *arXive e-print quant-ph/9811052,* 1998.

[BK99] S. L. Braunstein and H. J. Kimble. Dense coding for continuous variables. *arXive e-print quant-ph/9910010,* 1999.

[BKLW99] D. Bacon, J. Kempe, D. A. Lidar, and K. B. Whaley. Universal fault-tolerant computation on decoherence-free subspaces. *arXive e-print quant-ph/9909058,* 1999.

[BKN98] H. Barnum, E. Knill, and M. A. Nielsen. On quantum fidelities and channel capacities. *arXive e-print quant-ph/9809010,* 1998

[BL95] D. Boneh and R. J. Lipton. Quantum cryptoanalysis of hidden linear functions (extended abstract). In Don Coppersmith, editor, *Lecture notes in computer science — Advances in Cryptology — CRYPTO'95*, pages 424-437, Springer-Verlag, Berlin, 1995.

[BMP+99] P. O. Boykin, T. Mor, M. Pulver, V. Roychowdhury, and F. Vatan. On universal and fault-tolerant quantum computing. *arXive e-print quant-ph/9906054,* 1999.

[BNS98] H. Barnum, M. A. Nielsen, and B. W. Schumacher. Information transmission through a noisy quantum channel. *Phys. Rev. A,* 57: 4153, 1998.

[Boh51] D. Bohm. *Quantum Theory.* Prentice-Hall, Englewood Cliffs, New Jersey, 1951.

[BP93] S. M. Barnett and S. J. D. Phoenix. Information-theoretic limits to quantum cryptography. *Phys. Rev. A,* 48(1): R5-R8, 1993.

[BPM+97] D. Bouwmeester, J. W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger. Experimental quantum teleportation. *Nature,* 390 (6660): 575-579, 1997.

[BR98] D. S. Bethune and W. P. Risk. An autocompensating quantum key distribution system using polarization splitting of light. In *IQEC '98 Digest of Postdeadline Papers,* pages QPD12-2, Optical Society of America, Washington, DC, 1998.

[BR00] D. S. Bethune and W. P. Risk. An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light. *J. Quantum Electronics,* 36(3): 100, 2000.

[Bra93] G. Brassard. A bibliography of quantum cryptography. *Université de Montréal preprint,* pages 1-10, 3 December 1993. A preliminary version of this appeared in *Sigact News,* vol. 24(3), 1993, pages 16-20.

[Bra98] S. L. Braunstein. Error correction for continuous quantum variables. *Phys. Rev. Lett.,* 80: 4084-4087, 1998. *arXive e-print quant-ph/9711049.*

[BS94] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In T. Helleseth, editor, *Lecture Notes in Computer Science: Advances in Cryptology - EUROCRYPT'93,* Volume 765, pages 410-423, Springer-Verlag, New York, 1994.

[BS98] C. H. Bennett and P. W. Shor. Quantum information theory. *IEEE Trans. Inf. Theory,* 44(6): 2724-42, 1998.

[BST98] H. Barnum J. A. Smolin, and B. Terhal. Quantum capacity is properly defined without encodings. *Phys. Rev. A,* 58(5): 3496-3501, 1998.

[BT97] B. M. Boghosian and W. Taylor. Simulating quantum mechanics on a quantum computer. *arXive e-print quant-ph/9701019,* 1997.

[BV97] E. Bernstein and U. Vazirani. Quantum complexity theory. *SIAM J. Comput.,* 26(5): 1411-1473, 1997. *arXive e-print quant-ph/9701001* .

[BW92] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states. *Phys. Rev. Lett.,* 69(20): 2881-2884, 1992.

[CAK98] N. J. Cerf, C. Adami, and P. Kwiat. Optical simulation of quantum logic. *Phys. Rev. A,* 57: R1477, 1998.

[Cav99] C. M. Caves. Quantum error correction and reversible operations. *Journal of Superconductivity,* 12(6): 707-718, 1999.

[CD96] R. Cleve and D. P. DiVincenzo. Schumacher's quantum data compression as a quantum computation. *Phys. Rev. A,* 54: 2636, 1996. *arXive e-print quant-ph/9603009.*

[CEMM98] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca. Quantum algorithms revisited. *Proc. R. Soc. London A,* 454(1969): 339-354, 1998.

[CFH97] D . G. Cory, A. F . Fahmy, and T. F . Havel. Ensemble quantum computing by NMR spectroscopy. *Proc. Nat. Acad. Sci. USA,* 94: 1631-1639, 1997.

[CGK98] I. L. Chuang, N. Gershenfeld and M. Kubinec. Experimental implementation of fast quantum searching. *hys. Rev. Lett.,* 18(15): 3408-3411, 1998.

[CGKL98] I. L. Chuang, N. Gershenfeld, M. G. Kubinec, and D. W. Leung. Bulk quantum computation with nuclear-magnetic-resonance: theory and experiment. *Proc. R. Soc. London A*, 454(1969): 447-467, 1998.

[Che68] P. R. Chernoff. Note on product formulas for operator semigroups. *J. Functional Analysis,* 2: 238-242, 1968.

[Cho75] M.-D. Choi. Completely positive line maps on complex matrices. *Linear Algebra and Its Applications,* 10: 285-290, 1975.

[CHSH69] J. F. Clauser, M. A. Horne, A. Shimor and R. A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.,* 49: 1804-l807, 1969.

[Chu36] A. Church. An unsolvable problem of ementary number theory. *Am. J. Math.* (reprinted in [Dav65]), 58: 345, 1936.

[CK81] I. Csiszár and J. Körner. *Information Theory: Coding Theorems for Discrete Memoryless Systems.* Academic Press, New York, 1981.

[CL83] A. O. Caldeira and A. J. Leggett. Quantum tunnelling in a dissipative system. *Ann. Phys.,* 149(2): 371-456, 1983.

[Cla89] M. Clausen. Fast generalized Fourier transforms. *Theor. Comput. Sci.,* 67: 55-63, 1989.

[Cle99] R. Cleve. The query complexity of order-finding. *arXive e-print quant-ph/9911124,* 1999.

[CLR90] T. H. Cormen, C. E. Leiserson, R. L. Rivest. *Introduction to Algorithms.* MIT Press, Cambridge, Mass., 1990.

[CM97] C. Cachin and U. M. Maurer. Linking information reconciliation and privacy amplification. *J. Cryptology,* 10: 97-110, 1997.

[CM00] I. L. Chuang and D. Modha. Reversible arithmetic coding for quantum data compression. *IEEE Trans. Inf. Theory,* 46(3): 1104, May 2000.

[CMP+98] D. G. Cory, W. Mass, M. Price, E. Knill, R. Laflamme, W. H. Zurek, T. F. Havel, and S. S. Somaroo. Experimental quantum error correction. *arXive e-print quant-ph/9802018,* 1998.

[CN97] I. L. Chuang and M. A. Nielsen. Prescription for experimental determination of the dynamics of a quantum black box. *J. Mod. Opt.,* 44(11-12): 2455-2467, 1997. *arXive e-print quant-ph/9610001.*

[Con72] J. H. Conway. Unpredictable iterations. In *Proceedingd of the Number Theory Conference*, pages 49-52, Boulder, Colorado, 1972.

[Con86] J. H. Conway. Fractran: a simple universal programming language. In T. M. Cover and B. Gopinath, editors, *Open Probles in Communication and Computation*, pages 4-26, Springer-Verlag, New York, 1986.

[Coo71] S. A. Cook. The complexity of theorem-proving procedures. In *Proc. 3rd. Ann. ACM Symp. on Theory of Computing*, pages 151-158, Association for Computing Machinery, New York, 1971.

[Cop94] D. Coppersmith. An approximate Fourier transform useful in quantum factoring. *IBM Research Report RC 19642*, 1994.

[CPZ96] J. I. Cirac, T. Pellizzari, and P. Zoller. Enforcing coherent evolution in dissipative quantum dynamics. *Science,* 273: 1207, 1996.

[CRSS97] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction and orthogonal geometry. *Phys. Rev. Lett.,* 78: 405-8, 1997.

[CRSS98] A. R. Calderbank, E. M. Rains, P. W. Shor, and N. J. A. Sloane. Quantum error correction via codes over GF(4). *IEEE Trans. Inf. Theory,* 44(4): 1369-1387, 1998.

[CS96] A. R. Calderbank and P. W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A,* 54: 1098, 1996. *arXive e-print quant-ph/ 9512032.*

[CST89] R. A. Campos, B. E. A. Saleh, and M. C. Tiech. Quantum-mechanical lossless beam-splitters: SU(2) symmetry and photon statistics. *Phys. Rev. A,* 40: 1371, 1989.

[CT91] T. M. Cover and J. A. Thomas. *Elements of Information Theory.* John Wiley and Sons, New York, 1991.

[CTDL77a] C. Cohen-Tannoudji, B. Diu, and F. Laloë . *Quantum Mechanics. Vol. I.* John Wiley and Sons, New York, 1977.

[CTDL77b] C. Cohen-Tannoudji, B. Diu, and F. Laloë . *Quantum Mechanics. Vol. II.* John Wiley and Sons, New York, 1977.

[CVZ+98] I. L. Chuang, L. M. K. Vandersypen, X. L. Zhou, D. W. Leung, and S. Lloyd. Experimental realization of a quantum algorithm. *Nature,* 393(6681): 143-146, 1998.

[CW95] H. F. Chau and F. Wilczek. Simple realization of the Fredkin gate using a series of two-body operators. *Phys. Rev. Lett.,* 75(4): 748-50, 1995. *arXive e-print quant-ph/9503005.*

[CY95] I. L. Chuang and Y. Yamamoto. Simple quantum computer. *Phys. Rev. A,* 52: 3489-3496, 1995. *arXive e-print quant-ph/9505011.*

[CZ95] J. I. Cirac and P. Zoller. Quantum computations with cold trapped ions. *Phys. Rev. Lett.,* 74: 4091, 1995.

[Dav65] M. D. Davis, *The Undecidable.* Raven Press, Hewlett, New York, 1965.

[Dav76] E. B. Davis. *Quantum Theory of Open Systems.* Academic Press, London, 1976.

[DBE95] D. Deutsch, A. Barenco, and A. Ekert. Universality in quantum computation. *Proc. R. Soc. London A,* 449(1937): 669-677, 1995.

[Deu83] D. Deutsch. Uncertainty in quantum measurements. *Phys. Rev. Lett.,* 50(9): 631-633, 1983.

[Deu85] D. Deutsch. Quantum theory, the Church-Turing Principle and the universal quantum computer. *Proc. R. Soc. Lond. A, 400: 97, 1985.*

[Deu89] D. Deutsch. Quantum computational networks. *Proc. R. Soc. London A,* 425: 73, 1989.

[DG98] L.-M. Duan and G.-C. Guo. Probabilistic cloning and identification of linearly independent quantum states. *Phys. Rev. Lett.,* 80: 4999-5002, 1998. *arXive e-print quant-ph/9804064.*

[DH76] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Trans. Inf. Theory,* IT-22(6): 644-54, 1976.

[DH96] C. Dürr and P. Høyer. A quantum algorithm for finding the minimum. *arXive e-print quant-ph/9607014,* 1996.

[Die82] D. Dieks. Communication by EPR devices. *Phys. Lett. A,* 92(6): 271-272, 1982.

[DiV95a] D. P. DiVincenzo. Quantum computation. *Science,* 270: 255, 1995.

[DiV95b] D. P. DiVincenzo. Two-bit gates are universal for quantum computation. *Phys. Rev. A,* 51(2): 1015-1022, 1995.

[DiV98] D. P. DiVincenzo. Quantum gates and circuits. *Proc. R. Soc. London A,* 454: 261-276, 1998.

[DJ92] D. Deutsch and R. Jozsa. Rapid solution of problems by quantum computation. *Proc. R. Soc. London A,* 439: 553, 1992.

[DL98] W. Diffie and S. Landau. *Privacy on the Line: the Politics of Wiretapping and Encryption.* MIT Press, Cambridge Massachusetts, 1998.

[DMB+93] L. Davidovich, A. Maali, M. Brune, J. M. Raimond, and S. Haroche. *Phys. Rev. Lett.,* 71: 2360, 1993.

[DR90] P. Diaconis and D. Rockmore. Efficient computation of the Fourier transform on finite groups. *J. Amer. Math. Soc.,* 3(2): 297-332, 1990.

[DRBH87] L. Davidovich, J. M. Raimond, M. Brune, and S. Haroche. *Phys. Rev. A,* 36: 3771, 1987.

[DRBH95] P. Domokos, J. M. Raimond, M. Brune, and S. Haroche. Simple cavity-QED two-bit universal quantum logic gate: The principle and expected performances. *Phys. Rev. Lett.,* 52: 3554, 1995.

[DS96] D. P. DiVincenzo and P. W. Shor. Fault-tolerant error correction with efficient quantum codes. *Phys. Rev. Lett.,* 77: 3260, 1996.

[DSS98] D. P. DiVincenzo, P. W. Shor, and J. Smolin. Quantum-channel capacities of very noisy channels. *Phys. Rev. A,* 57(2): 830-839, 1998.

[Ear42] S. Earnshaw. On the nature of the molecular forces which regulate the constitution of the luminiferous ether. *Trans. Camb. Phil. Soc.,* 7: 97-112, 1842.

[EBW87] R. R. Ernst, G. Bodenhausen, and A. Wokaun. *Principles of Nuclear Magnetic Resonance in One and Two Dimensions.* Oxford University Press, Oxford, 1987.

[EH99] M. Ettinger and P. Høyer. On quantum algorithms for noncommutative hidden subgroups. In *Symposium on Theoretical Aspects in Computer Science.* Universitv of Trier, 1999. *arXive e-print quant-ph/9807029.*

[EHK99] M. Ettinger, P. Høyer, and E. Knill. Hidden subgroup states are almost orthogonal. *arXive e-print quant-ph/9901034,* 1999.

[EHPP94] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres. Eavesdropping on quantum-cryptographical systems. *Phys. Rev. A,* 50(2): 1047-1056, 1994.

[EJ96] A. Ekert and R. Jozsa. Quantum computation and Shor's factoring algorithm. Rev. Mod. Phys., 68: 733, 1996.

[EJ98] A. Ekert and R. Jozsa. Quantum algorithm: Entanglement enhanced information prosessing. *Proc. R. Soc. London A,* 356(1743): 1769-82, Aug. 1998. *arXive e-print quant-ph/803072.*

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.,* 67(6): 661-663, 1991.

[EM96] A. Ekert and C. Macchiavello. Error correction in quantum communication. *Phys. Rev. Lett.,* 77: 2585, 1996. *arXive e-print quant-ph/9602022.*

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.,* 47: 777-780, 1935.

[Eps73] H. Epstein. *Commun. Math. Phys.* 31: 317-325, 1973.

[Fan73] M. Fannes. A continuity property of the entropy density for spin lattice systems. *Commun. Math. Phys.,* 31: 291-294, 1973.

[FC94] C. A. Fuchs and C. M. Caves. Ensemble-dependent bounds for accessible information in quantum mechanics. *Phys. Rev. Lett.,* 73(23): 3047-3050, 1994.

[Fel68a] W. Feller. *An Introduction to Probability Theory and its Applications,* Volume 1. Wiley, New York, 1968.

[Fel68b] W. Feller. *An Introduction to Probability Theory and its Applications,* Volume 2. Wiley. New York, 1968.

[Fey82] R. P. Feynman. Simulating physics computers. *Int. J. Theor. Phys.,* 21: 467, 1982.

[FG98] E. Farhi and S. Gutmann. An analog analogue of a digital quantum computation. Phys. Rev. A, 57(4): 2403-2406, 1998. *arXive e-print quant-ph/9612026.*

[FLS65a] R. P. Feynman, R. B. Leighton, M. Sands. Volume III of *The Feynman Lectures on Physics.* Addison-Wesley, Reading, Mass., 1965.

[FLS65b] R. P. Feynman. R. B. Leighton, M. Sands. Volume I of *The Feynman Lectures on Phvsics.* Addison-Wesley, Reading, Mass., 1965.

[FM98] M. H. Freedman and D. A. Meyer. Projective plane and planar quantum codes. *arXive e-print quant-ph/9810055,* 1998.

[FS92] A. Fässler and E. Stiefel. *Group Theoretical Methods and Their Applications.* Birhaüser, Boston, 1992.

[FSB+98] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik. Unconditional quantum teleportation. *Science,* 282: 706-709, 1998.

[FT82] E. Fredkin and T. Toffoli. Conservative logic. *Int. J. Theor. Phys.,* 21(3/4): 219-253, 1982.

[Fuc96] C. A. Fuchs. *Distinguishability and Accessible Information in Quantum Theory.* Ph.D. thesis, The University of New Mexico, Albuquerque, NM, 1996. *arXive e-print quant-ph/9501020.*

[Fuc97] C. A. Fuchs. Nonorthogonal quantum states maximize classical informatin capacity. *Phys. Rev. Lett.,* 79(6): 1162-1165, 1997.

[FvdG99] C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory,* 45(4): 1216-1227, 1999.

[Gar91] C. W. Gardiner. *Quantum Noise.* Springer-Verlag, Berlin, 1991.

[GC97] N. Gershenfeld and I. L. Chuang. Bulk spin resonance quantum computation. *Science,* 275: 350, 1997.

[GC99] D. Gottesman and I. L. Chuang. Quantum teleportation is a universal computational primitive. *Nature,* 402: 390-392, 1999. *arXive e-print quant-ph/9908010.*

[GJ79] M. R. Garey and D. S. Johnson. *Computers and Intractibility.* W. H. Freeman and Company, New York, 1979.

[GN96] R. B. Griffiths and C.-S. Niu. Semiclassical Fourier transform for quantum computation. *Phys. Rev. Lett.,* 76(17): 3228-3231, 1996. arXive e-print quant-ph/9511007.

[Gor64] J. P. Gordon. Noise at optical frequencies; information theory. In P. A. Miles, editor, *Quantum Electronics and Coherent Light,* Proceedings of the International School of Physics 'Enrico Fermi' XXXI, Academic Press, New York, 1964.

[Got96] D. Gottesman. Class of quantum error-correcting codes saturating the quantum Hamming bound. *Phys. Rev. A,* 54: 1862, 1996.

[Got97] D. Gottesman. *Stabilizer Codes and Quantum Error Correction.* Ph.D. thesis, California Institute of Technology, Pasadena, CA, 1997.

[Got98a] D. Gottesman. Fault-tolerant quantum computation with higher- dimensional systems. *arXive e-print quant-ph/9802007,* 1998.

[Got98b] D. Gottesman. Theory of fault-tolerant quantum computation. *Phys. Rev. A,* 57(1): 127-137, 1998. *arXive e-print quant-ph/9702029.*

[GP10] D. Gottesman and J. Preskill. The Hitchiker's guide to the threshold theorem. Eternally in preparation, 1: 1-9120, 2010.

[Gro96] L. Grover. In *Proc. 28th Annual ACM Symposium on the Theory of Computation,* pages 212-219, ACM Press, New York, 1996

[Gro97] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.,* 79(2): 325, 1997. *arXive e-print quant-ph/9706033.*

[Gru99] J. Gruska. *Quantum Computing.* McGraw-Hill, London, 1999. ヨゼフ・グルスカ原著, 伊藤正美・今井克暢・岩本宙造・外山政文・森田憲一共訳 「量子コンピューティング」 森北出版, 2003.

[GS92] G. R. Grimmett and D. R. Stirzaker. *Probability and Random Processes.* Clarendon Press, Oxford, 1992.

[HAD+95] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer. Quantum cryptography. *Contemp. Phys.,* 36(3): 149-163, 1995. *arXive e-print quant-ph/9504002.*

[Hal58] P. R. Halmos. *Finite-dinrensional Vector Spaces.* Van Nostrand, Princeton, N.J., 1958.

[Ham89] M. Hammermesh. *Group Theory and its Application to Physical Problems.* Dover, New York, 1989.

[HGP96] J. L. Hennessey, D. Goldberg, and D. A. Patterson. *Computer Architecture: A Quantitative Approach.* Academic Press, New York, 1996.

[HHH96] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A,* 223(1-2): 1-8, 1996.

[HHH98] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and distillation: is there a 'bound' entanglement in nature? *Phys. Rev. Lett.*, 80(24): 239-5242, 1998.

[HHH99a] M. Horodecki, P. Horodecki, and R. Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A,* 60(3): 1888-1898, 1999 .

[HHH99b] M. Horodecki, P. Horodecki, and R. Horodecki. Limits for entanglement measures. *arXive e-print quant-ph/9908065, 1999.*

[HHH99c] P. Horodecki, M. Horodecki, and R. Horodecki. Bound entanglement can be activated. *Phys. Rev. Lett.*, 82(5): 1056-1059, 1999.

[HJ85] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge University Press, Cambridge, 1985.

[HJ91] R. A. Horn and C. R. Johnson. *Topics in Matrix Analysis.* Cambridge University Press, Cambridge, 1991.

[HJS+96] P. Hausladen, R. Jozsa, B. Schumacher, M. Westmoreland, and W. K. Wootters. Classical information capacity of a quantum channel. *Phys. Rev. A,* 54: 1869, 1996.

[HJW93] L. P. Hughston, R. Jozsa, and W. K. Wootters. A complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A,* 183: 14-18, 1993.

[HK69] K.-E. Hellwig and K. Kraus. Pure operations and measurements. *Commun. Math. Phys.*, 11: 214-220, 1969.

[HK70] K.-E. Hellwig and K. Kraus. Operations and measurements. II. *Commun. Math. Phys.*, 16: 142-147, 1970.

[Hof79] D. R. Hofstadter. *Gödel. Escher. Bach: an Eternal Golden Braid.* Basic Books, New York, 1979.

[Hol73] A. S. Holevo. Statistical problems in quantum physics. In Gisiro Maruyama and Jurii V. Prokhorov, editors, *Proceedings of the Second Japan-USSR Symposium on Probability Theory,* pages 104-119, Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, vol. 330.

[Hol79] A. S. Holevo. Capacity of a quantum communications channel. *Problems of Inf. Transm.*, 5(4): 247-253, 1979.

[Hol98] A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory,* 44(1): 269-273, 1998.

[Hor97] M. Horodecki. Limits for compression of quantum information carried by ensembles of mixed states. *Phys. Rev. A,* 57: 3364-3369, 1997.

[HSM+98] A. G. Huibers, M. Switkes, C. M. Marcus, K. Campman, and A. C. Gossard. Dephasing in open quantum dots. *Phys. Rev. Lett.*, 82: 200, 1998.

[HW60] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers. Fourth Edition.* Oxford University Press, London, 1960.

[IAB+99] A. Imamoglu, D. D. Awschalom, G. Burkard, D. P. DiVincenzo, D. Loss, M. Sherwin, and A. Small. Quantum information processing using quantum dot spins and cavity QED. *Phys. Rev. Lett.*, 83(20): 4204-7, 1999.

[IY94] A. Imamoglu and Y. Tamamoto. Turnstile device for heralded single photons: Coulomb blockade of electron and hole tunneling in quantum confined p-i-n heterojunctions. *Phys. Rev. Lett.*, 72(2): 210-13, 1994.

[Jam98] D. James. The theory of heating of the quantum ground state of trapped ions. *arXive e-print quant-ph/9804048,* 1998.

[Jay57] E. T. Jaynes. Information theory and statistical mechanics. ii. *Phys. Rev.*, 108(2): 171-190, 1957.

[JM98] J. A. Jones and M. Mosca. Implementation of a quantum algorithm to solve Deutsch's problem on a nuclear magnetic resonance quantum computer. *arXive e-print quant-ph/9801027*, 1998.

[JMH98] J. A. Jones, M. Mosca, and R. H. Hansen. Implementation of a quantum search algorithm on a nuclear magnetic resonance quantum computer. *Nature*, 393(6683): 344, 1998. *arXive e-print quant-ph/9805069.*

[Jon94] K. R. W. Jones. Fundamental limits upon the measurement of state vectors. *Phys. Rev. A*, 50: 3682-3699, 1994.

[Joz94] R. Jozsa. Fidelity for mixed quantum states. *J. Mod. Opt.*, 41: 2315-2323, 1994.

[Joz97] R. Jozsa. Quantum algorithms and the Fourier transform. *arXive e-print quant-ph/9707033*, 1997.

[JP99] D. Jonathan and M. B. Plenio. Entanglement-assisted local manipulation of pure states. *Phys. Rev. Lett.*, 83: 3566-3569, 1999.

[JS94] R. Jozsa and B. Schumacher. A new proof of the quantum noiseless coding theorem. *J. Mod. Opt.*, 41: 2343-2349, 1994.

[Kah96] D. Kahn. *Codebreakers: the Story of Secret Writing.* Scribner, New York, 1996.

[Kan98] B. Kane. A silicon-based nuclear spin quantum computer. *Nature*, 393: 133-137, 1998.

[Kar72] R. M. Karp. Reducibility among combinatorial problems. In *Complexity of Computer Computations*, pages 85-103, Plenum Press, New York, 1972.

[KCL98] E. Knill, I. Chuang, and R. Laflamme. Effective pure states for bulk quantum computaion. *Phys. Rev. A*, 57(5): 3348-3363, 1998. *arXive e-print quant-ph/9706053.*

[Kit95] A. Y. Kitaev. Quantum measurements and the Abelian stabilizer problem. *arXive e-print quant-ph/9511026*, 1995.

[Kit97a] A. Y. Kitaev. Fault-tolerant quantum computation by anyons. *arXive e-print quant-ph/9707021*, 1997.

[Kit97b] A. Y. Kitaev. Quantum computations: algorithm and error correction. *Russ. Math. Surv.*, 52(6): 1191-1249, 1997.

[Kit97c] A. Y. Kitaev. Quantum error correction with imperfect gates. In A. S. Holevo, O. Hirota, and C. M. Caves, editors, *Quantum Communication, Computing, and Measurement*, pages 181-188, Plenum Press, New York, 1997.

[KL51] S. Kullback and R. A. Leibler. On information and sufficiency. *Ann. Math. Stat.*, 22: 79-86, 1951.

[KL97] E. Knill and R. Laflamme. A theory of quantum error-correcting codes. *Phys. Rev. A*, 55: 900, 1997. *arXive e-print quant-ph/9604034.*

[KL99] E. Knill and R. Laflamme. Quantum computation and quadratically signed weight enumerators. *arXive e-print quant-ph/9909094*, 1999.

[Kle31] O. Klein. *Z. Phys.*, 72: 767-775, 1931.

[KLV99] E. Knill, R. Laflamme, and L. Viola. Theory of quantum error correction for general noise. *arXive e-print quant-ph/9908066*, 1999.

[KLZ98a] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation. *Science*, 279(5349): 342-345, 1998. *arXive e-print quant-ph/9702058.*

[KLZ98b] E. Knill, R. Laflamme, and W. H. Zurek. Resilient quantum computation: error models and thresholds. *Proc. R. Soc. London A*, 454(1969): 365-384, 1998. *arXive e-print quant-ph/9702058.*

[KMSW99] P. G. Kwiat, J. R. Mitchell, P. D. D. Schwindt, and A. G. White. Grover's search algorithm: An optical approach. *arXive e-print quant-ph/9905086*, 1999.

[Kni95] E. Knill. Approximating quantum circuits. *arXive e-print quant-ph/9508006*, 1995.

[Knu97] D. E. Knuth. *Fundamental Algorithms 3rd Edition*, Volume 1 of *The Art of Computer Programming.* Addison-Wesley, Reading, Massachusetts, 1997.

[Knu98a] D. E. Knuth. *Seminumerical Algorithms 3rd Edition,* Volume 2 of *The Art of Computer Programming.* Addison-Wesley, Reading, Massachusetts, 1998.

[Knu98b] D. E. Knuth. *Sorting and Searching 2nd Edition,* Volume 3 of *The Art of Computer Programming.* Addison-Wesley, Reading, Massachusetts, 1998.

[Kob94] N. Koblitz. *A Course in Number Theory aand Cryptography.* Springer-Verlag, New York, 1994.

[KR99] C. King and M. B. Ruskai. Minimal entropy of states emerging from noisy quantum channels. *arXive e-print quant-ph/9911079,* 1999

[Kra83] K. Kraus. *States, Effects, and Operations: Fundamental Notions of Quantum Theory.* Lecture Notes in Physics, Vol. 190. Springer-Verlag, Berlin, 1983.

[Kra87] K. Kraus. Complementary observables and uncertainty relations. *Phys. Rev. D,* 35(10): 3070-3075, 1987.

[KSC+94] P. G. Kwiat, A. M. Steinberg, R. Y. Chiao, P. H. Eberhard, and M. D. Petroff. Absolute efficiency and time-response measurement of single-photon detectors. *Appl. Opt.,* 33(10): 1844-1853, 1994.

[KU91] M. Kitagawa and M. Ueda. Nonlinear-interferometric generation of number-phase correlated Fermion states. *Phys. Rev. Lett.,* 67(14): 1852, 1991.

[Lan27] L. Landau. Das dampfungsproblem in der wellenmechanik. *Z. Phys.,* 45: 430-441, 1927.

[Lan61] R. Landauer. Irreversibility and heat generation in the computing process. *IBM J. Res. Dev.,* 5: 183, 1961.

[LB99] S. Lloyd and S. Braunstein. Quantum computation over continuous variables. *Phys. Rev. Lett.,* 82: 1784-1787, 1999. *arXive e-print quant-ph/9810082.*

[LBW99] D. A. Lidar, D. A. Bacon, and K. B. Whaley. Concatenating decoherence free subspaces with quantum error correcting codes. *Phys. Rev. Lett.,* 82(22): 4556-4559, 1999.

[LC99] H. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science,* 283: 2050-2056, 1999. *arXive e-print quant-ph/9803006.*

[LCW98] D. A. Lidar, I. L. Chuang, and K. B. Whaley. Decoherence-free subspaces for quantum computation. *Phys. Rev. Lett.,* 81(12): 2594-2597, 1998.

[LD98] D. Loss and D. P. DiVincenzo. Quantum computation with quantum dots. *Phys. Rev. A,* 57: 120-126, 1998.

[Lee63] Y. Lecerf. Machines de Turing réversibles. *Comptes Rendus,* 257: 2597-2600, 1963.

[Leo97] U. Leonhardt. *Measuring the Quantum State of Light.* Cambridge University Press, New York, 1997.

[Lev73] L. Levin. Universal sorting problems. *Probl. Peredaci Inf.,* 9: 115-116, 1973. Original in Russian. English translation in *Probl. Inf. Transm. USSR* 9: 265-266 (1973).

[Lie73] E. H. Lieb. Convex trace functions and the Wigner-Yanase-Dyson conjecture. *Ad. Math.,* 11: 267-288, 1973.

[Lie75] E. H. Lieb. *Bull. AMS,* 81: 1-13, 1975.

[Lin75] G. Lindblad. Completely positive maps and entropy inequalities. *Commun. Math. Phys.,* 40: 147-151, 1975.

[Lin76] G. Lindblad. On the generators of quantum dynamical semigroups. *Commun. Math. Phys.,* 48: 199, 1976.

[Lin91] G. Lindblad. Quantum entropy and quantum measurements. In C. Bendjaballah, O. Hirota, and S. Reynaud, editors, *Quantum Aspects of Optical Communications,* Lecture Notes in Physics, vol. 378, pages 71-80, Springer-Verlag, Berlin, 1991.

[Lip95] R. Lipton. DNA solution of hard computational problems. *Science,* 268: 542-525, 1995.

[LKF99] N. Linden, E. Kupce, and R. Freeman. NMR quantum logic gates for homonuclear spin systems. *arXive e-print quant-ph/9907003,* 1999.

[LL93] A. K. Lenstra and H. W. Lenstra Jr., editors. *The Development of the Number Field Sieve.* Springer-Verlag, New York, 1993.

[Llo93] S. Lloyd. A potentially realizable quantum computer. *Science,* 261: 1569, 1993.

[Llo94] S. Lloyd. Necessary and sufficient conditions for quantum computation. *J. Mod. Opt.,* 41(12): 2503, 1994.

[Llo95] S. Lloyd. Almost any quantum logic gate is universal. *Phys. Rev. Lett.,* 75(2): 346, 1995.

[Llo96] S. Lloyd. Universal quantum simulators. *Science,* 273: 1073, 1996.

[Llo97] S. Lloyd. The capacity of the noisy quantum channel. *Phys. Rev. A,* 56: 1613, 1997

[LLS75] R. E. Ladner, N. A. Lynch, and A. L. Selman. A comparison of polynomial-time reducibilities. *Theor. Comp. Sci.,* 1: 103-124, 1975.

[LMPZ96] R. Laflamme, C. Miquel, J.-P. Paz, and W. H. Zurek. Perfect quantum error correction code. *Phys. Rev. Lett.,* 77: 198, 1996. *arXive e-print quant-ph/9602019.*

[LNCY97] D. W. Leung, M. A. Nielsen, I. L. Chuang, and Y. Yamamoto. Approximate quantum error correction can lead to better codes. *Phys. Rev. A*, 56: 2567-2573, 1997. *arXive e-print quant-ph/9704002.*

[Lo99] H. Lo. A simple proof of the unconditional security of quantum key distribution. *arXive e-print quant-ph/9904091,* 1999.

[Lom87] J. S. Lomont. *Applications of Finite Groups.* Dover, New York, 1987.

[Lou73] W. H. Louisell. *Quantum Statistical Properties of Radiation.* Wiley, New York, 1973.

[LP97] H.-K. Lo and S. Popescu. Concentrating local entanglement by local actions — beyond mean values. *arXive e-print quant-ph/9707038,* 1997.

[LP99] N. Linden and S. Popescu. Good dynamics versus bad kinematics. Is entanglement needed for quantum computation? *arXive e-print quant-ph/9906008,* 1999.

[LR68] O. E. Lanford and D. Robinson. Mean entropy of states in quantum-statistical mechanics. *J. Math. Phys.,* 9(7): 1120-1125, 1968.

[LR73a] E. H. Lieb and M. B. Ruskai. A fundamental property of quantum-mechanical entropy. *Phys. Rev. Lett.,* 30(10): 434-436, 1973.

[LR73b] E. H. Lieb and M. B. Ruskai. Proof of the strong subadditivity of quantum mechanical entropy. *J. Math. Phys.,* 14: 1938-1941, 1973.

[LR90] H. Leff and R. Rex. *Maxwell's Demon: Entropy, Information, Computing.* Princeton University Press, Princeton, NJ, 1990.

[LS93] L. J. Landau and R. F. Streater. On Birkhoff theorem for doubly stochastic completely positive maps of matrix algebras. *Linear Algebra Appl.,* 193: 107-127, 1993.

[LS98] S. Lloyd and J. E. Slotine. Analog quantum error correction. *Phys. Rev. Lett.,* 80: 4088-4091, 1998.

[LSP98] H.-K. Lo, T. Spiller, and S. Popescu. *Quantum information and computation.* World Scientific, Singapore, 1998.

[LTV98] M. Li, J. Tromp, and P. Vitanyi. Reversible simulation of irreversible computation by pebble games. *Physica D,* 120: 168-176, 1998.

[LV96] M. Li and P. Vitanyi. Reversibility and adiabatic computation: trading time and space for energy. *Proc. R. Soc. London A,* 452: 769-789, 1996. *arXive e-print quant-ph/9703022.*

[LVZ+99] D. W. Leung, L. M. K. Vandersypen, X. Zhou, M. Sherwood, C. Yannoni, M. Kubinec, and I. L. Chuang. Experimental realization of a two-bit phase damping quantum code. *Phys. Rev. A,* 60: 1924, 1999.

[Man80] Y. Manin. *Computable and Uncomputable (in Russian)* . Sovetskoye Radio, Moscow, 1980.

[Man99] Y. I. Manin. Classical computing, quantum computing, and Shor's factoring algorithm. *arXive e-print quant-ph/9903008,* 1999.

[Mau93] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theory,* 39: 733-742, 1993.

[Max71] J. C. Maxwell. *Theory of Heat.* Longmans, Green, and Co., London, 1871.

[May98] D. Mayers. Unconditional security in quantum cryptography. *arXive e-print quant-ph/9802025,* 1998.

[ME99] M. Mosca and A. Ekert. The hidden sub-group problem and eigenvalue estimation on a quantum computer. *arXive e-print quant-ph/9903071,* 1999.

[Mer78] R. Merkle. Secure communications over insecure channels. *Comm. of the ACM,* 21: 294-299, 1978.

[Mil76] G. L. Miller. Riemann's hypothesis and tests for primality. *J. Comput. Syst. Sci.,* 13(3): 300-317, 1976.

[Mil89a] G. J. Milburn. Quantum optical Fredkin gate. *Phys. Rev. Lett.,* 62(18): 2124, 1989.

[Mil89b] D. A. B. Miller. Optics for low energy communications inside digital processors: quantum detectors, sources, and modulators as efficient impedance converters. *Opt. Lett.,* 14: 146, 1989.

[Mil96] G. J. Milburn. A quantum mechanical Maxwell's demon. Unpublished, 1996.

[Mil97] G. J. Milburn. *Schrödinger's Machines: the Quantum Technology Reshaping Everyday Llfe.* W. H. Freeman. New York, 1997.

[Mil98] G. J. Milburn. *The Feynman Processor: Quantum Entanglement and the Computing Revolution.* Perseus Books, Reading, Mass., 1998.

[Min67] M. L. Minsky. *Computation: finite and infinite machines.* Prentice-Hall, Englewood Cliffs, N. J., 1967.

[MM92] M. Marcus and H. Minc. *A Survey of Matrix Theory and Marix Inequalities.* Dover, New York, 1992.

[MMK+95] C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland. Demonstration of a fundamental quantum logic gate. *Phys. Rev. Lett.,* 75: 4714, 1995.

[MO79] A. W. Marshall and I. Olkin. *Inequalities: Theory of Majorization and its Applications.* Academic Press, New York, 1979.

[MOL+99] J. E. Mooij, T. P. Orlando, L. Levitov, L. Tian, C. H. van der Waal, and S. Lloyd. Josephson persistent-current qubit. *Science,* 285: 1036-1039, 1999.

[Mor98] T. Mor. No-cloning of orthogonal states in composite systems. *Phys. Rev. Lett.,* 80: 3137-3140, 1998.

[Mos98] M. Mosca. Quantum searching, counting and amplitude amplification by eigenvector analysis. In R. Freivalds, editor, *Proceedings of International Workshop on Randomized Algorithms,* pages 90-100, 1998.

[Mos99] M. Mosca. *Quantum Computer Algorithms.* Ph.D. thesis, University of Oxford, 1999.

[MR95] R. Motwani and P. Raghavan. *Randomized Algorithms.* Cambridge University Press, Cambridge, 1995.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-correcting Codes.* North-Holland, Amsterdam, 1977.

[MU88] H. Maassen and J. H. B. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.,* 60(12): 1103-1106, 1988.

[MvOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[MWKZ96] K. Mattle, H. Weinfurter, P. G. Kwiat, and A. Zeilinger. Dense coding in experimental quantum communication. *Phys. Rev. Lett.,* 76(25): 4656-4659, 1996.

[MZG96] A. Muller. H. Zbinden, and N. Gisin. Quantum cryptography over 23 km in installed under-lake telecom fibre. *Europhys. Lett.*, 33: 334-339, 1996.

[NC97] M. A. Nielsen and C. M. Caves. Reversible quantum operations and their application to teleportation. *Phys. Rev. A*, 55(4): 2547-2556, 1997.

[NCSB98] M. A. Nielsen, C. M. Caves, B. Schumacher, and H. Barnum. Information-theoretic approach to quantum error correction and reversible measurement. *Proc. R. Soc. London A*, 454(1969): 277-304, 1998.

[Nie98] M. A. Nielsen. *Quantum Information Theory*. Ph.D. thesis, University of New Mexico, 1998.

[Nie99a] M. A. Nielsen. Conditions for a class of entanglement transformations. *Phys. Rev. Lett.*, 83(2): 436-439, 1999.

[Nie99b] M. A. Nielsen. Probability distributions consistent with a mixed state. *arXive e-print quant-ph/9909020*, 1999.

[NKL98] M. A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation using nuclear magnetic resonance. *Nature*, 396(6706): 52-55, 1998.

[NPT99] Y. Nakamura, Y. A. Pashkin, and J. S. Tsai. Coherent control of macroscopic quantum states in a single-cooper-pair box. *Nature*, 398: 786-788, 1999.

[OP93] M. Ohya and D. Petz. *Quantum Entropy and Its Use*. Springer-Verlag, Berlin, 1993.

[Pai82] A. Pais. *Subtle is the Lord: The Science and the Llfe of Albert Einstein*. Oxford University Press, Oxford, 1982.

[Pai86] A. Pais. *Inward Bound: Of Matter and Forces in the Physical World*. Oxford University Press, Oxford, 1986.

[Pai91] A. Pais. *Niels Bohr's Times: In Physics, Philosophy, and Polity*. Oxford University Press, Oxford, 1991.

[Pap94] C. M. Papadimitriou. *Computational Complexity*. Addison-Wesley, Reading, Massachusetts, 1994.

[Pat92] R. Paturi. On the degree of polynomials that approximate symmetric Boolean functions (preliminary version). *Proc. 24th Ann. ACM Symp. on Theory of Computing (STOC '92)*, pages 468-474, 1992.

[PCZ97] J. F. Poyatos, J. I. Cirac, and P. Zoller. Complete characterization of a quantum process: the two-bit quantum gate. *Phys. Rev. Lett.*, 78(2): 390-393, 1997.

[PD99] P. M. Platzman, and M. I. Dykman. Quantum computing with electrons floating on liquid helium. *Science*, 284: 1967, 1999.

[Pen89] R. Penrose. *The Emperor's New Mind*. Oxford University Press, Oxford, 1989.

[Per52] S. Perlis. *Theory of Matrices*. Addison-Wesley, Reading, Mass., 1952.

[Per88] A. Peres. How to differentiate between non-orthogonal states. *Phys. Lett. A*, 128: 19, 1988.

[Per93] A. Peres. *Quantum Theory: Concepts and Methods*. Kluwer Academic, Dordrecht, 1993.

[Per95] A. Peres. Higher order Schmidt decompositions. *Phys. Lett. A*, 202: 16-17, 1995.

[Pet86] D. Petz. Quasi-entropies for finite quantum systems. *Rep. Math. Phys.*, 23(1): 57-65, 1986.

[Phy92] Physics Today Editor. Quantum cryptography defies eavesdropping. *Physics Today*, page 21, November 1992.

[PK96] M. B. Plenio and P. L. Knight. Realistic lower bounds for the factorization time of large numbers on a quantum computer. *Phys. Rev. A*, 53: 2986-2990, 1996.

[PK98] M. B. Plenio and P. L. Knight. The quantum-jump approach to dissipative dynamics in quantum optics. *Rev. Mod. Phys.*, 70(1): 101-144, 1998.

[Pop75] R. P. Poplavskii. Thermodynamical models of information processing (in Russian). *Usp. Fiz. Nauk,* 115(3): 465-501, 1975.

[PRB98] M. Pueschel, M. Roetteler, and T. Beth. Fast quantum Fourier transforms for a class of non-abelian groups. *arXive e-print quant-ph/9807064,* 1998.

[Pre97] J. Preskill. Fault-tolerant quantum computation. *arXive e-print quant-ph/9712048,* 1997.

[Pre98a] J. Preskill. Fault-tolerant quantum computation. In H.-K. Lo, T. Spiller, and S. Popescu, editors, *Quantum information and computation.* World Scientific, Singapore, 1998.

[Pre98b] J. Preskill. *Physics 229: Advanced Mathematical Methods of Physics — Quantum Computation and Information.* California Institute of Technology, 1998.
URL: http://www.theory.caltech.edu/people/preskill/ph229/

[Pre98c] J. Preskill. Reliable quantum computers. *Proc. R. Soc. London A,* 454(1969): 385-410 1998.

[Rab80] M. O. Rabin. Probabilistic algorithm for testing primarity. *J. Number Theory,* 12: 128-138, 1980.

[Rah99] H. Z. Rahim. Richard Feynman and Bill Gates: an imaginary encounter. 1999.
URL: http://www.trnsoft.com/features/1rfbg.htm

[Rai98] E. M. Rains. Quantum weight enumerators. *IEEE Trans. Inf. Theory,* 44(4): 1388-1394, 1998.

[Rai99a] E. M. Rains. Monotonicity of the quantum linear pragramming bound. *IEEE Trans. Inf. Theory,* 45(7): 2489-2492, 1999.

[Rai99b] E. M. Rains. Nonbinary quantum codes. *IEEE Trans. Inf. Theory,* 45(6): 1827-1832, 1999.

[Rai99c] E. M. Rains. Quantum shadow enumerators. *IEEE Trans. Inf. Theory,* 45(7): 2361-2366, 1999.

[RB98] M. Roetteler and T. Beth. Polynomial-time solution to the hidden subgroup problem for a class of non-abelian groups. *arXive e-print quant-ph/9812070,* 1998.

[Res81] A. Ressler. *The Design of a Conservative Logic Computer and A Graphical Editor Simulator.* Master's thesis, Massachusetts Institute of Technology, 1981.

[RHSS97] E. M. Rains, R. H. Hardin, P. W. Shor, and N. J. A. Sloane. Nonadditive quantum code. *Phys. Rev. Lett.,* 79(5): 953-954, 1997.

[Roy96] A. Royer. Reduced dynamics with initial correlations, and time-dependent environment and Hamiltonians. *Phys. Rev. Lett.,* 77(16): 3272-3275, 1996.

[RR67] D. W. Robinson and D. Ruelle. *Commun. Math. Phys.,* 5: 288, 1967.

[RSA78] R. L. Rivest, A. Shamir, and L. M. Adleman. A method of obtaining digital signatures and public-key cryptosystems. *Comm. ACM,* 21(2): 120-126, 1978.

[Rus94] M. B. Ruskai. Beyond strong subadditivity: improved bounds on the contraction of generalized relative entropy. *Rev. Math. Phys.,* 6(5A): 1147-1161, 1994.

[RWvD84] S . Ramo , J. R. Whinnery , and T. van Duzer. *Fields and waves in communication electronics.* Wiley, New York, 1984.

[RZBB94] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.,* 73(1): 58-61, 1994.

[Sak95] J. J. Sakurai. *Modern Quantum Mechanics.* Addison-Wesley, Reading, Mass., 1995.

[SC99] R. Schack and C. M. Caves. Classical model for bulk-ensemble NMR quantum computation. *Phys. Rev. A,* 60(6): 4354-4362, 1999.

[Sch06] E. Schmidt. Zur theorie der linearen und nichtlinearen integralgleighungen. *Math. Annalen.,* 63: 433-476, 1906.

[Sch36] E. Schrödinger. Probability relations between separated system. *Proc. Cambridge Philos. Soc.*, 32: 446-452, 1936.

[Sch95] B. Schumacher. Quantum codng. *Phys. Rev. A*, 51: 2738-2747, 1995.

[Sch96a] B. Schneier. *Applied Cryptography.* John Wiley and Sons, New York, 1996.

[Sch96b] B. W. Schumacher. Sending entanglement through noisy quantum channels. *Phys. Rev. A*, 54: 2614, 1996.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Tech. J.*, 27: 379-423, 623-656, 1948.

[Sho94] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings, 35th Annual Symposium on Foundations of Computer Science,* IEEE Press, Los Alamitos, CA, 1994.

[Sho95] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Phys. Rev. A*, 52: 2493, 1995.

[Sho96] P. W. Shor. Fault-tolerant quantum computation. In *Proceedings, 37th Annual Symposium on Foundation of Computer Science,* pages 56-65, IEEE Press, Los Alamitos, CA, 1996.

[Sho97] P. W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comp.*, 26(5): 1484-1509, 1997.

[Sim79] B. Simon. *Trace Ideals and Their Applications.* Cambridge University Press, Cambridge, 1979.

[Sim94] D. Simon. On the power of quantum computation. In *Proceedings. 35th Annual Symposium on Foundations of Computer Science,* pages 116-123, IEEE Press, Los Alamitos, CA, 1994.

[Sim97] D. R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5): 1474-1483, 1997.

[SL97] P. W. Shor and R. Laflamme. Quantum analog of the MacWilliams identities for classical coding theory. *Phys. Rev. Lett.*, 78(8): 1600-1602, 1997.

[SL98] D. Shasha and C. Lazere. *Out of Their Minds: The Lives and Discoveries of 15 Great Computer Scientists.* Springer-Verlag, New York, 1998.

[Sle74] D. Slepian, editor. *Keys Papers in the Development of Information Theory.* IEEE Press, New York, 1974.

[Sli96] C. P. Slichter. *Principles of Magnetic Resonance.* Springer, Berlin, 1996.

[SN96] B. W. Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Phys. Rev. A*, 54(4): 2629, 1996. *arXive e-print quant-ph/9604022.*

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *arXive e-print quant-ph/0003004*, 2000.

[SS76] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Comput.*, 6: 84-85, 1976.

[SS96] P. W. Shor and J. A. Smolin. Quantum error-correcting codes need not completely reveal the error syndrome. *arXive e-print quant-ph/9604006,* 1996.

[SS99] A. T. Sornborger and E. D. Stewart. Higher order methods for simulations on quantum computers. *Phys. Rev. A*, 60(3): 1956-1965, 1999. *arXive e-print quant-ph/9903055.*

[ST91] B. E. A. Saleh and M. C. Teich. *Fundamentals of Photonics.* Wiley, NY, 1991.

[Ste96a] A. M. Steane. Error correcting codes in quantum theory. *Phys. Rev. Lett.*, 77: 793, 1996.

[Ste96b] A. M. Steane. Multiple particle interference and quantum error correction. *Proc. R. Soc. London A*, 452: 2551-76, 1996.

[Ste97] A. Steane. The ion-trap quantum information processor. *Appl . Phys. B - Lasers and Optics,* 64(6): 623-642, 1997.

[Ste99] A. M. Steane. Efficient fault-tolerant quantum computing. *Nature,* 399: 124-126, May 1999.

[STH+99] S. Somaroo, C. H. Tseng, T. F. Havel, R. Laflamme, and D. G. Cory. Quantum simulations on a quantum computer. *Phys. Rev. Lett.,* 82: 5381-5384, 1999.

[Str76] G. Strang. *Linear Algebra and Its Applications.* Academic Press, New York, 1976.

[SV99] L. J. Schulman and U. Vazirani. Molecular scale heat engines and scalable quantum computation. *Proc. 31st Ann. ACM Symp. on Theory of Computing (STOC '99),* pages 322-329, 1999.

[SW49] C. E. Shannon and W. Weaver. *The Mathematical Theory of Communication.* University of Illinois Press, Urbana, 1949.

[SW93] N. J. A. Sloane and A. D. Wyner, editors. *Claude Elwood Shannon: Collected Papers.* IEEE Press, New York, 1993.

[SW97] B. Schumacher and M. D. Westmoreland. Sending classical information via noisy quantum channels. *Phys. Rev. A,* 56(1): 131-138, 1997.

[SW98] B. Schumacher and M. D. Westmoreland. Quantum privacy and quantum coherence. *Phys. Rev. Lett.,* 80(25): 5695-5697, 1998.

[SWW96] B. W. Schumacher, M. Westmoreland, and W. K. Wootters. Limitation on the amount of accessible information in a quantum channel. *Phys. Rev. Lett.,* 76: 3453, 1996.

[Szi29] L. Szilard. Uber die entropieverminderung in einen thermodynamischen system bei eingriffen intelligenter wesen. *Z. Phys.,* 53: 840-856, 1929.

[TD98] B. M. Terhal and D. P. DiVincenzo. The problem of equilibration and the computation of correlation functions on a quantum computer. *arXive e-print quant-ph/9810063,* 1998.

[THL+95] Q. A. Turchette, C. J. Hood, W. Lange, H. Mabuchi, and H. J. Kimble. Measurement of conditional phase shifts for quantum logic. *Phys. Rev. Lett.,* 75: 4710, 1995.

[Tro59] H. F. Trotter. On the product of semigroups of operators. *Proc. Am. Math. Soc.,* 10: 545-551, 1959.

[Tsi80] B. S. Tsirelson. Quantum generalizations of Bell's inequality. *Lett. Math. Phys.,* 4: 93, 1980.

[Tur36] A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proc. Lond. Math. Soc. 2* (reprinted in [Dav65]), 42: 230, 1936.

[Tur97] Q. A. Turchette. *Quantum optics with single atoms and single photons.* Ph.D. thesis, California Institute of Technology, Pasadena, California, 1997.

[Uhl70] A. Uhlmann. On the Shannon entropy and related functionals on convex sets. *Rep. Math. Phys.,* 1(2): 147-159, 1970.

[Uhl71] A. Uhlmann. Sätze über dichtematrizen. *Wiss. Z. Karl-Marx-Univ. Leipzig,* 20: 633-637, 1971.

[Uhl72] A. Uhlmann. Endlich-dimensionale dichtermatrizen I. *Wiss. Z. Karl-Marx-Univ. Leipzig,* 21: 421-452, 1972

[Uhl73] A. Uhlmann. Endlich-dimensionale dichtermatrizen II. *Wiss. Z. Karl-Marx-Univ. Leipzig,* 22: 139-177, 1973

[Uhl76] A. Uhlmann. The 'Transition probability' in the state space of a *-algebra. *Rep. Math. Phys.,* 9: 273-279, 1976.

[Uhl77] A. Uhlmann. Relative entropy and the Wigner-Yanase-Dyson-Lieb concavity in an interpolation theory. *Commun. Math. Phys.,* 54: 21-32, 1977.

[Ume62] H. Umegaki. *Kōdai Math. Sem. Rep.,* 14: 59-85, 1962.

[Vai94] L. Vaidman. Teleportation of quantum states. *Phys. Rev. A,* 49(2): 1473-6, 1994.

[van98a] W. van Dam. Quantum oracle interrogation: getting all information for half the price. In *Proceedings of the 39th FOCS,* 1998. *arXive e-print quant-ph/9805006.*

[van98b] S. J. van Enk. No-cloning and superluminal signaling. *arXive e-print quant-ph/9803030,* 1998.

[Ved99] V. Vedral. Landauer's erasure, error correction and entanglement. *arXive e-print quant-ph/9903049,* 1999.

[Vid98] G. Vidal. Entanglement monotones. *arXive e-print quant-ph/9807077,* 1998 .

[Vid99] G. Vidal. Entanglement of pure states for a single copy. *Phys. Rev. Lett.,* 83(5): 1046-1049, 1999.

[von27] J. von Neumann. *Göttinger Nachrichten,* page 245, 1927.

[von56] J. von Neumann. Probabilistic logics and the synthesis of reliable organisms from unreliable components. In *Automata Studies,* pages 329-378, Princeton University Press, Princeton, NJ, 1956.

[von66] J. von Neumann. Fourth University of Illinois lecture. In A. W. Burks, editor, *Theory of Self-Reproducing Automata,* page 66, University of Illinois Press, Urbana, 1966.

[VP98] V. Vedral and M. B. Plenio. Entanglement measures and purification procedures. *Phys. Rev. A,* 57(3): 1619-1633, 1998.

[VR89] K. Vogel and H. Risken. Determination of quasiprobability distributions in terms of probability distributions for the rotated quadrature phase. *Phys. Rev. A,* 40(5): 2847-2849, 1989.

[VYSC99] L. M. K. Vandersypen, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang. Realization of effective pure states for bulk quantum computation. *Phys. Rev. Lett.,* 83: 3085-3088, 1999.

[VYW+99] R. Vrijen, E. Yablonovitch, K. Wang, H. W. Jiang, A. Balandin, V. Roychowdhury, T. Mor, and D. DiVincenzo. Electron spin resonance transistors for quantum computing in silicon-germanium
heterostructures. *arXive e-print quant-ph/9905096,* 1999

[War97] W. Warren. The usefulness of NMR quantum computing. *Science*, 277(5332): 1688, 1997.

[Wat99] J. Watrous. **PSPACE** has 2-round quantum interactive proof systems. *arXive e-print cs/9901015,* 1999.

[WC67] S. Winograd and J. D. Cowan. *Reliable Computation in the Presence of Noise.* MIT Press, Cambridge, MA, 1967.

[Weh78] A. Wehrl. General properties of entropy. *Rev. Mod. Phys.,* 50: 221, 1978.

[Wel88] D. J. A. Welsh. *Codes and Cryptography.* Oxford University Press, New York, 1988.

[Wie] S. Wiesner. Unpublished manuscript, circa 1969, appeared as [Wie83].

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News,* 15: 77, 1983.

[Wie96] S. Wiesner. Simulations of many-body quantum systems by a quantum computer. *arXive e-print quant-ph/9603028,* 1996.

[Wil91] D. Williams. *Probability with Martingales.* Cambridge University Press, Cambridge, 1991.

[Win98] E. Winfree. *Algorithmic Self-Assembly of DNA.* Ph.D. thesis, California Institute of Technology, Pasadena, California, 1998.

[WMI+98] D. J. Wineland, C. Monroe, W. M. Itano, D. Leibfried, B. E. King, and D. M. Meekhof. Experimental issues in coherent quantum-state manipulation of trapped atomic ions. *J. Res. Natl. Inst. Stand. Tech.,* 103: 259, 1998.

[WS98] M. D. Westmoreland and B. Schumacher. Quantum entanglement and the non-existence of superluminal signals. *arXive e-print quant-ph/9801014,* 1998.

[WY63] E. P. Wigner and M. M. Yanase. *Proc. Natl. Acad. Sci. (U.S.A.),* 49: 910-918, 1963.

[WY90] K. Watanabe and Y. Yamamoto. Limits on tradeoffs between third-order optical nonlinearity, absorption loss, and pulse duration in self-induced transparency and real excitation. *Phys. Rev. A,* 42(3): 1699-702, 1990.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature,* 299: 802-803, 1982.

[Yao93] A. C. Yao. Quantum circuit complexity. *Proc. of the 34th Ann. IEEE Symp. on Foundations of Computer Science,* pages 352-361, 1993.

[YK95] S. Younis and T. Knight. Non dissipative rail drivers for adiabatic circuits. In *Proceedings. Sixteenth Conference on Advanced Research in VLSI 1995,* pages 404-14, IEEE Computer Society Press, Los Alamitos, CA, 1995.

[YKI88] Y. Yamamoto. M. Kitagawa, and K. Igeta. In *Proc. 3rd. Asia-Pacific Phys. Conf.,* World Scientific, Singapore, 1988.

[YO93] H. P. Yuen and M. Ozawa. Ultimate information carrying limit of quantum systems. *Phys. Rev. Lett.,* 70: 363-366, 1993.

[YY99] F. Yamaguchi and Y. Yamamoto. Crystal lattice quantum computer. *Appl. Phys. A,* pages 1-8, 1999.

[Zal98] C. Zalka. Simulating quantum systems on a quantum computer. *Proc. R. Soc. London A,* 454(1969): 313-322, 1998.

[Zal99] C. Zalka. Grover's quantum searching algorithm is optimal. *Phys. Rev. A,* 60(4): 2746-2751, 1999.

[Zan99] P. Zanardi. Stabilizing quantum information. *arXive e-print quant-ph/9910016,* 1999.

[ZG97] P. Zoller and C. W. Gardiner. Quantum noise in quantum optics: the stochastic Schrödinger equation. In S. Reynaud, E. Giacobino, and J. Zinn-Justin, editors) *Quantum Fluctuations: Les Houches Summer School LXIII,* Elsevier, Amsterdam, 1997.

[ZHSL99] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein. Volume of the set of separable states. *Phys. Rev. A,* 58(2): 883-892, 1999.

[ZL96] W. H. Zurek and R. Laflamme. Quantum logical operations on encoded qubits. Phys. Rev. Lett., 77(22): 4683-4686, 1996.

[ZLC00] X. Zhou, D. W. Leung, and I. L. Chuang. Quantum logic gate constructions with one-bit "teleportation". *arXive e-print quant-ph/0002039,* 2000.

[ZR98] P. Zanardi and M. Rasetti. Noiseless quantum codes. *Phys. Rev. Lett.,* 79(17): 3306-3309, 1998.

[Zur89] W. H. Zurek. Thermodynamic cost of computation, algorithmic complexity and the information metric. *Nature,* 341: 119, 1989 .

[Zur91] W. H. Zurek. Decoherence and the transition from quantum to classical. *Phys. Today,* October 1991.

索　引

〈著者・訳者の紹介〉

Michael A. Nielsen（ミカエル ニールセン）

現在，クイーンズランド大学において量子情報研究財団の教授とオーストラリア研究協議連盟のフェローを務める．出身はオーストラリアのブリスベン．クイーンズランド大学で数学と物理学の大学院を修了した後，米国ニューメキシコ大学においてFulbright奨学生となり物理学の学位を取得．その後，カリフォルニア工科大学でTolmanポストドクター研究員を務め，2000年にオーストラリアに戻り現職．

Isaac L. Chuang（アイザック チャン）

現在マサチューセッツ工科大学（MIT）・物理学部の準教授．同大学メディア研究所のビットと原子研究センターにおいて量子情報科学研究グループを率いる．出身はケンタッキー州ルイズビル．スタンフォード大学においてHertz財団フェローとなり，電気工学の学位を取得．さらにMITから物理学と電気工学の学位も得る．趣味は読書，ハイキングおよびバイオリンの演奏．

木 村 達 也（きむら たつや）

東京大学大学院工学系研究科を修了，工学博士の学位を取得．NTT研究所において光伝送方式，光ファイバ，光部品に関する基礎研究を進め，長波長帯光ファイバ伝送や光増幅中継等の先端的光ファイバ通信を提唱．その後，材料物性および情報科学の基礎研究マネジメントに従事して，量子光学，ナノサイエンス，情報科学の研究を推進し，NTT理事・基礎研究所長，NEC支配人を歴任．現在NTTアドバンステクノロジ(株)シニアアドバイザを務める．IEEEフェロー，IEICEフェロー，OSA名誉会員．

量子コンピュータと量子通信 I ―量子力学とコンピュータ科学―

平成16年12月20日　第1版第1刷発行

著　者　Michael A. Nielsen
　　　　Isaac L. Chuang
訳　者　木 村 達 也
発行者　佐 藤 政 次
発行所　株式会社 オ ー ム 社
　　　　郵便番号　101-8460
　　　　東京都千代田区神田錦町3-1
　　　　電 話　03(3233)0641(代表)
　　　　URL　http://www.ohmsha.co.jp/

印刷　中央印刷　　製本　三水舎
ISBN4-274-20007-8　Printed in Japan